CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

# NATIONAL CYBER SECURITY
## FRAMEWORK MANUAL

EDITED BY
ALEXANDER KLIMBURG

*This publication is supported by:* The NATO Science for Peace and Security Programme

This publication may be cited as:
Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,
Tallinn 2012

© 2012 by NATO Cooperative Cyber Defence Centre of Excellence

All rights reserved. No part of this publication may be reprinted, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the NATO Cooperative Cyber Defence Centre of Excellence (publications@ccdcoe.org). This restriction does not apply to making digital or hard copies of this publication for internal use within NATO, and for personal or educational use when for non-profit or non-commercial purposes, providing that copies bear a full citation.

**PRINTED COPIES OF THIS PUBLICATION ARE AVAILABLE FROM:**

NATO CCD COE Publications
Filtri tee 12, 10132 Tallinn, Estonia
**Phone:** +372 717 6800
**Fax:** +372 717 6308
**E-mail:** publications@ccdcoe.org
**Web:** www.ccdcoe.org

**LEGAL NOTICE**

This publication contains opinions of the respective authors only. They do not necessarily reflect the policy or the opinion of NATO CCD COE, NATO, or any agency or any government. NATO CCD COE may not be held responsible for any loss or harm arising from the use of information contained in this book and is not responsible for the content of the external sources, including external websites referenced in this publication.

Print: OÜ Greif Trükikoda
Cover design & content layout: Marko Söönurm

ISBN 978-9949-9211-1-9 (print)
ISBN 978-9949-9211-2-6 (pdf)
ISBN 978-9949-9211-3-3 (epub)

# NATIONAL CYBER SECURITY
## FRAMEWORK MANUAL

EDITED BY

ALEXANDER KLIMBURG

*NATO Cooperative Cyber Defence Centre of Excellence*

# ABOUT THE NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, and the USA as Sponsoring Nations. The Centre is not part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

The NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO Member States and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-orientated, interdisciplinary approach to its key activities, including: academic research on selected topics relevant to the cyber domain from legal, policy, strategic, doctrinal and/or technical perspectives; providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultancy upon request.

For more information on the NATO CCD COE, please visit the Centre's website at http://www.ccdcoe.org.

For information on Centres of Excellence, visit NATO's website 'Centres of Excellence' at http://www.nato.int/cps/en/natolive/topics_68372.htm.

# ACKNOWLEDGEMENTS

Special gratitude for contributions to the discussions during workshops supporting the elaboration of this publication is owed to:

*Jart Armin*, CEO, CyberDefcon and Editor, HostExploit

Prof Dr *Paul Cornish*, Professor of International Security, University of Bath

Prof Dr *Chris Demchak*, US Naval War College, Strategic Research Department/ NWC Center for Cyber Conflict Studies

*Maeve Dion*, Institute for Law & IT, Faculty of Law, Stockholm University

*Yurie Ito*, Director, Global Coordination, JPCERT/CC

*John C. Mallery*, Research Scientist, Computer Science & Artificial Intelligence Laboratory, Massachusetts Institute of Technology (MIT)

*Philipp Mirtl*, Fellow and Adviser, Austrian Institute for International Affairs (oiip)

*Jeff Moss*, Vice President and Chief Security Officer, Internet Corporation for Assigned Names and Numbers (ICANN)

*Greg Rattray,* CEO and Founding Partner, Delta Risk LLC

LTC *Jan Stinissen* (NLD-A), Legal & Policy Branch, NATO CCD COE

*Heli Tiirmaa-Klaar*, Cyber Security Advisor, Security Policy and Conflict Prevention Directorate, European External Action Service, EU

The participants of the workshops are not responsible for the contents of this publication, as the final decision in regard to the content was taken by the editor in coordination with the NATO CCD COE.

# CONTENTS

**Foreword** ..... X

**Introduction** ..... XII

**Executive Summary** ..... XV

**1. Preliminary Considerations: On National Cyber Security** ..... 1
*Melissa E. Hathaway, Alexander Klimburg*

**1.1. Introduction** ..... 1
1.1.1. Cyber: Converging Dependencies ..... 2
1.1.2. The Cost of Connectivity ..... 4

**1.2. Cyber Terms and Definitions** ..... 8
1.2.1. Information, ICT, and Cyber Security ..... 9
1.2.2. Cyber Crime ..... 13
1.2.3. Cyber Espionage ..... 16
1.2.4. 'Cyber Warfare' ..... 17

**1.3. National Cyber Security** ..... 20
1.3.1. Comparison of 'National' and 'Cyber' Security ..... 20
1.3.2. Cyber Power and National Security ..... 27

**1.4. Conceptualising National Cyber Security** ..... 29
1.4.1. The Three Dimensions: Governmental, National and International ..... 29
1.4.2. The Five Mandates of National Cyber Security ..... 31

**1.5. The Five Dilemmas of National Cyber Security** ..... 34
1.5.1. Stimulate the Economy vs. Improve National Security ..... 34
1.5.2. Infrastructure Modernisation vs. Critical Infrastructure Protection ..... 36
1.5.3. Private Sector vs. Public Sector ..... 37
1.5.4. Data Protection vs. Information Sharing ..... 39
1.5.5. Freedom of Expression vs. Political Stability ..... 41

**1.6. Conclusion** ..... 42

**2. Political Aims & Policy Methods** ..... 44
*Gustav Lindstrom, Eric Luiijf*

**2.1. Introduction** ..... 44
2.1.1. Aims of National Security Strategies ..... 45
2.1.2. Trends in National Security Strategy Formulation ..... 47
2.1.3. Integrating Cyber Security in National Security Strategies ..... 51

**2.2. The National Cyber Security Dimension** ..... 53

2.2.1. Themes in National Cyber Security Strategies ..... 53
2.2.2. Aims and Addressees ..... 58
2.3. Implementing Cyber Security Strategies ..... 59
2.3.1. The Use of Terms ..... 59
2.3.2. The Role of Transparency ..... 60
2.3.3. Addressing Stakeholders ..... 61
2.4. Political Pitfalls, Frictions and Lessons Identified ..... 63

3. Strategic Goals & Stakeholders ..... 66
*Alexander Klimburg, Jason Healey*
3.1. Introduction ..... 67
3.1.1. National Cyber Security Actors ..... 67
3.1.2. National Cyber Security Advantages ..... 71
3.1.3. Offensive Actions in Cyber ..... 74
3.1.4. Defensive Actions in Cyber ..... 78
3.1.5. Collective Cyber Defence ..... 81
3.2. Strategic Concepts: Balancing Defensive and Offensive ..... 81
3.2.1. 'Deterrence': Cost Imposed ..... 82
3.2.2. 'Resilience': Benefit Denied ..... 84
3.3. Two Tensions of National Cyber Security ..... 86
3.3.1. Military vs. Civilian Approaches ..... 86
3.3.2. The Law Enforcement vs. Intelligence Community Approaches ..... 87
3.4. Strategy Development Processes ..... 89
3.4.1. Bottom-Up, Top-Down and Re-Iterative ..... 89
3.4.2. Governmental vs. Societal Approaches ..... 91
3.4.3. Resources, Budgets and Metrics ..... 93
3.5. Engagement with Stakeholders ..... 94
3.5.1. Whole of Government (WoG) ..... 95
3.5.2. Whole of Nation (WoN) ..... 96
3.5.3. Whole of System (WoS) ..... 99
3.5.4. National Cyber Security: Coordinate, Cooperate and Collaborate ..... 101
3.6. Strategic Pitfalls, Frictions and Lessons Identified ..... 103

4. Organisational Structures & Considerations ..... 108
*Eric Luiijf, Jason Healey*
4.1. Introduction ..... 109
4.2. Delineating Organisational Functions, Capabilities and Responsibilities ..... 109
4.2.1. Across the Levels of Government ..... 110

4.2.2. Across the Incident Management Cycle ... 112
4.3. Cyber Security Stakeholders ... 114
4.4. Main Focus of Analysis ... 116
4.4.1. Along the Mandates ... 116
4.4.2. Along the Cross-Mandates ... 119
4.5. The Five Mandates of National Cyber Security ... 120
4.5.1. Military Cyber Operations ... 121
4.5.2. Counter Cyber Crime ... 122
4.5.3. Intelligence/Counter-Intelligence ... 123
4.5.4. Cyber Security Crisis Management and CIP ... 124
4.5.5. Internet Governance and Cyber Diplomacy ... 127
4.6. The Three Cross-Mandates Activities ... 129
4.6.1. Coordination ... 130
4.6.2. Information Exchange and Data Protection ... 132
4.6.3. Research & Development and Education ... 133
4.7. International Cyber Security Organisations ... 134
4.7.1. Government-Focused Activities ... 135
4.7.2. Nation-Focused Activities ... 137
4.7.3. System-Focused Activities ... 138
4.8. Organisational Pitfalls, Frictions and Lessons Identified ... 140

5. Commitments, Mechanisms & Governance ... 146
*Victoria Ekstedt, Tom Parkhouse, Dave Clemente*
5.1. Introduction ... 146
5.2. Nature of State Commitments ... 149
5.2.1. Legal Commitments ... 150
5.2.2. Cyber-Enabled Terrorism ... 155
5.2.3. Cyber Espionage ... 157
5.2.4. Cyber Criminality ... 158
5.2.5. Convention on Cybercrime ... 160
5.2.6. Human Rights ... 163
5.2.7. International Humanitarian Law ... 166
5.2.8. Legal Thresholds ... 168
5.3. Interpretation of Commitments ... 170
5.3.1. Governance ... 171
5.3.2. Assurance Mechanisms: Information Security ... 175
5.4. NATO's Cyber Dimension ... 180
5.4.1. NATO's Collective/Cyber Defence ... 182

5.4.2. Cooperation with Non-NATO Nations ... 185
5.4.3. NATO-EU Cooperation ... 186
5.4.4. The NATO Defence Planning Process ... 187
5.5. Conclusion ... 188
5.6. Tactical/Technical Pitfalls, Frictions and Lessons Identified ... 189
6. Conclusion ... 191
6.1. The Road so Far ... 191
6.2. Final Remarks ... 195
Annex: List of Principal Guidelines ... 196
Bibliography ... 203
Glossary ... 225
Authors' Biographies ... 233

## Figures

Figure 1: Relationship between Cyber Security and other Security Domains ... 10
Figure 2: Parsing Cyber Offense ... 78
Figure 3: The Four Levels of War as a Generalised Tool for Analysis ... 111
Figure 4: The Five Mandates and the Six Elements of the Cyber Security Incident Cycle Model ... 118
Figure 5: The Cross-Mandates and the Six Elements of the Cyber Security Incident Cycle Model ... 120
Figure 6: The Organisational Picture Across Mandates ... 129
Figure 7: The Organisational Picture of the Cross-Mandates ... 134

## Tables

Table 1: The Core Theoretical Approaches ... XVI
Table 2: Today and the Near Future ... 4
Table 3: National (Cyber) Security Strategies in Selected OECD Countries ... 23
Table 4: Comparison of Threats and Vulnerabilities ... 48
Table 5: Examples of National Cyber Security Strategies ... 53
Table 6: Differences Between WoG, WoN and WoS ... 100

# FOREWORD

Information and communications technologies have become indispensable to the modern lifestyle. We depend on information and communications infrastructure in governing our societies, conducting business, and exercising our rights and freedoms as citizens. In the same way, nations have become dependent on their information and communications infrastructure and threats against its availability, integrity and confidentiality can affect the very functioning of our societies.

The security of a nation's online environment is dependent on a number of stakeholders with differing needs and roles. From the user of public communications services to the Internet Service Provider supplying the infrastructure and handling everyday functioning of services, to the entities ensuring a nation's internal and external security interests – every user of an information system affects the level of resistance of the national information infrastructure to cyber threats. Successful national cyber security strategies must take into consideration all the concerned stakeholders, the need for their awareness of their responsibilities and the need to provide them with the necessary means to carry out their tasks. Also, national cyber security cannot be viewed as merely a sectoral responsibility: it requires a coordinated effort of all stakeholders. Therefore, collaboration is a common thread that runs through most of the currently available national strategies and policies.

Moreover, the different national cyber security strategies represent another common understanding: while national policies are bound by the borders of national sovereignty, they address an environment based on both infrastructure and functioning logic that has no regard for national boundaries. Cyber security is an international challenge, which requires international cooperation in order to successfully attain an acceptable level of security on a global level.

National interests tend to have priority over common interests and this is an approach which may be difficult to change, if it needs changing at all. As long as we can find the common ground and discuss the problematic issues out in the open, national interests should not impede international cooperation.

The task of drafting a national cyber security strategy is a complex one. In addition to the versatile threat landscape and the various players involved, the measures to address cyber threats come from a number of different areas. They can be political, technological, legal, economic, managerial or military in nature, or can involve other disciplines appropriate for the particular risks. All of these competences need to come together to offer responses capable of strengthening security and resisting threats in unison, rather than in competition for a more prominent role or for resources. Also, any security measures foreseen must consistently be balanced

against basic rights and freedoms and their effects on the economic environment must be considered. In the end, it is important to understand that cyber security is not an isolated objective, but rather a system of safeguards and responsibilities to ensure the functioning of open and modern societies.

We believe that this Manual will provide not only an appreciation for all the facets that need to be considered in drafting a national cyber security strategy, but also genuine tools and highly competent advice for this process. It is our hope that the Manual will serve to further a higher level of cyber security both on the national and international levels.

Artur Suzik
Colonel, EST-A
NATO CCD COE
Director

Tallinn, Estonia
November 2012

# INTRODUCTION

As stated in the *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation* of November 2010, NATO Member States have recognised that malicious cyber activities 'can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability'.[1] In order to assure the security of NATO's territory and populations, the Alliance has committed to continue fulfilling its essential core tasks, *inter alia*, to deter and to defend against emerging security challenges, such as cyber threats.[2] The revised NATO *Policy on Cyber Defence* of 8 June 2011 focuses NATO on the protection of its own communication and information systems in order to perform the Alliance's core tasks of collective defence and crisis management.[3] However, as cyber threats transcend State borders and organisational boundaries, the policy also stresses the need for cooperation of the Alliance with NATO partner countries, private sector and academia.[4] NATO Member States reinforced the importance of international cooperation by stating in the *Chicago Summit Declaration* of May 2012 that '[t]o address the cyber security threats and to improve our common security, we are committed to engage with relevant partner countries on a case-by-case basis and with international organisations [...] in order to increase concrete cooperation.'[5]

Against this background, it is of paramount importance to increase the level of protection against cyber threats and to steadily improve the abilities to appropriately address cyber threats by Allies and NATO's partner countries. The 'National Cyber Security Framework Manual' addresses national cyber security stakeholders in NATO Member States or NATO partner countries, including leaders, legislators, regulators and Internet Service Providers. It will serve as a guide to develop, improve or confirm national policies, laws and regulations, decision-making processes and other aspects relevant to national cyber security. Hence, this Manual will support NATO's goal of enhancing the 'common security' with regard

---

1 Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, adopted by Heads of State and Government at the NATO in Lisbon 19-20 November 2010, at para. 12, available at http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

2 *Ibid*., at para 4.a); Defending the networks. The NATO Policy on Cyber Defence, available at http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

3 Defending the networks. The NATO Policy on Cyber Defence, available at http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

4 Information available at the NATO website 'NATO and cyber defence', available at http://www.nato.int/cps/en/SID-714ABCE0-30D8F09C/natolive/topics_78170.htm.

5 Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012, at para. 49, available at http://www.nato.int/cps/en/SID-D03EFAB6-46AC90F8/natolive/official_texts_87593.htm?selectedLocale=en.

to 'cyber security threats', as expressed by the Allies in the aforementioned *Chicago Summit Declaration*.

The implementation, maintenance and improvement of national cyber security comprises a range of elements. These can address strategic documents of political nature, laws, regulations, organisational and administrative measures, such as communication and crisis management procedures within a State, but also purely technical protection measures. Furthermore, awareness raising, training, education, exercises and international cooperation are important features of national cyber security. Thus, the aspects to be considered reach from the strategic through the administrative or operational to the tactical level. This Manual addresses all of those levels in the various sections, shows different possibilities of approaches to national cyber security, and highlights good practices within national cyber security strategies and techniques. This approach is based on the reasoning that States have different features and prerequisites with regard to their legal framework, historical and political contexts, governmental structure, organisational structures, crisis management processes, and mentality. Therefore, this Manual cannot provide a 'blueprint' which would be feasible and useful for all States, but rather shows diverse aspects and possibilities to be considered in the course of drafting a national cyber security strategy. Due to its rather academic approach – although being of practical use – and the incorporation of military aspects, the Manual differs from publications with a similar goal and target audience.

The editor and the authors of the manual are internationally recognised experts in the arena of cyber security and cyber defence, representing a diversity of nationalities and disciplines, and showing a variety of professional backgrounds and experience. Their biographies, which can be found at the end of this volume, provide a more detailed illustration of their expertise.

The publication was elaborated within the context of a project funded by the NATO's *Science for Peace and Security Programme* (NATO SPS Programme), 'a policy tool for enhancing cooperation and dialogue with all partners, based on civil science and innovation, to contribute to the Alliance's core goals and to address the priority areas for dialogue and cooperation identified in the new partnership policy'.[6] The project consisted of three workshops with the participation of experts from various disciplines and from different NATO Member States and partner countries. The workshops discussed, at high level and in a round-table setting, different national policy approaches to the cyber domain. The experts represented a supranational organisation (EU), diverse governmental agencies, including the military, academia,

6 See NATO SPS website, available at http://www.nato.int/cps/en/SID-51871B1B-CD538A0D/natolive/topics_85373.htm.

think tanks, private companies and NGOs. Many of them have extensive professional experience in advising governmental entities with regard to national cyber security or aspects thereof. The three workshops[7] directly supported the present publication by generating discussions between the experts gathered, including the authors of the manual and the NATO CCD COE project manager. This publication was funded by the aforementioned NATO SPS Programme.

We hope that this volume will prove to be a valuable tool supporting NATO Member States and NATO partner countries, as well as all stakeholders in cyber security, in improving their ability to appropriately address cyber threats. In this way, it will directly support NATO's strategic goal to improve the level of cyber defence within the geographic scope of the Alliance and its partner countries.

Last but not least, we would like to thank all the authors and the editor for their superb contributions and friendly cooperation in the course of the publication process.

Dr *Katharina Ziolkowski*
DEU-Civ
NATO CCD COE
Project Manager

Tallinn, Estonia
November 2012

7 The first workshop was held by NATO CCD COE in Austria in cooperation with the Austrian Institute for International Affairs. The second workshop was held in Sweden in cooperation with the Swedish Armed Forces Computer Network Operations Unit. The third workshop was conducted by NATO CCD COE in Geneva in cooperation with the Geneva Centre for Security Policy (GCSP).

# EXECUTIVE SUMMARY

The term 'national cyber security' is increasingly used in policy discussions, but hardly ever defined. In this, it is very similar to the wider subject of cyber security itself – where common interpretations and implied meanings are much more frequent than universally accepted and legally-binding definitions. In cyber security, as a rule, the individual national context will define the specific definitions, which in turn will define the specific approaches – there are very few fixed points in cyber security.

Accordingly, the 'National Cyber Security Framework Manual' does not strive to provide a single universally applicable checklist of things to consider when drafting a national cyber security strategy. Rather, it provides detailed background information and theoretical frameworks to help the reader understand the different facets of national cyber security, according to different levels of public policy formulation. The four levels of government – political, strategic, operational and tactical (technical) – each have their own perspectives on national cyber security, and each is addressed in individual sections. Additionally, throughout the Manual there are call-out boxes that give examples of relevant institutions in national cyber security, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions. The Manual can thus be read as a collective volume or on a section-by-section basis, according to the needs of the reader.

**Section 1 ('Preliminary Considerations')** provides an introduction to the general topic of national cyber security. Particular attention is paid to terms and definitions: the use of certain terms (such as 'cyber security' rather than 'internet security') is connected not only to different policy choices, but also develops out of fundamentally different world-views. National cyber security is examined in relation to various national definitions of cyber security and national security. Also, an overall definition of national cyber security is offered. Further, the overall theory is presented that national cyber security effectively amounts to the precarious equilibrium of various contradictory needs – effectively 'Five Dilemmas' – that need to be balanced.

**Section 2 ('Political Aims')** considers the role that national security plays at the top level of security policy formulation. Since the end of the Cold War, a number of new threats and risk factors have competed for the attention of policy-makers. Cyber security is only one of these new issues that need to be considered. However, there is an increasing shift towards seeing cyber security as one of the most important of these new challenges. An analysis of 20 national cyber security strategies shows that there are diverging definitions of both cyberspace and cyber security. While all

strategies understand the centrality of working with different stakeholders, many strategies lack effective engagement mechanisms for defining those relationships.

**Table 1:** The Core Theoretical Approaches

| | |
|---|---|
| **National Cyber Security (NCS)**<br><br>*Defined* | *'The focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security.'* |
| **The 5 Mandates**<br><br>*Different interpretations of NCS & common activities* | - Military Cyber<br>- Counter Cyber Crime<br>- Intelligence and Counter-Intelligence<br>- Critical Infrastructure Protection and National Crisis Management<br>- Cyber Diplomacy and Internet Governance<br>+ 3 'Cross Mandates': coordination, information exchange and data protection, research & development and education |
| **The 3 Dimensions**<br><br>*Different stakeholder groups in NCS* | - Governmental (central, state, local) – 'coordination'<br>- National (CIP/contactors, security companies, civil society) – 'co-operation'<br>- International (legal, political and industry frameworks) – 'collaboration' |
| **The 5 Dilemmas**<br><br>*Balancing the cost and benefits of NCS* | - Stimulate the Economy vs. Improve National Security<br>- Infrastructure Modernisation vs. Critical Infrastructure Protection<br>- Private Sector vs. Public Sector<br>- Data Protection vs. Information Sharing<br>- Freedom of Expression vs. Political Stability |

**Section 3 ('Strategic Goals')** evaluates key elements of cyber security within national security. The centrality of offensive and defensive activities in cyberspace, the variety of actors that engage in these activities, and the tensions that arise through various institutional heritages are examined from the perspective of developing strategic goals to fit a specific national security requirement. The importance of understanding different stakeholder groups in national cyber security is incorporated into a theory of the 'Three Dimensions' of cyber security – where governmental, societal and international stakeholders need to work together in order to succeed.

**Section 4 ('Organisational Considerations')** emphasises the 'Five Mandates' (or interpretations) of national cyber security and their over-arching cross-mandate activities. Each of the 'Five Mandates' has a different set of requirements and goals that need to be brought into proper relationship with each other. Moreover, three cross-mandates are highlighted. Adapting the incident management model

to these mandates, a possible distribution of cyber security-related tasks within a governmental framework is offered. Additionally, the importance of collaboration with a number of international organisations is highlighted as a key factor for effective national cyber security.

**Section 5 ('Commitments, Mechanisms and Governance')** explores some of the legal and governance frameworks for actually delivering operational national cyber security. In particular, relevant international agreements and regulations, such as the Council of Europe Convention on Cybercrime and the International Humanitarian Law, are examined with a view towards their implications for operational cyber security. The wider framework of NATO collaboration, both for Member States and partners, is considered as well.

**Section 6 ('Conclusion')** summarises some of the previous points, and illustrates the need for national cyber security in both developing and developed nations, even though the very concept is likely to change in the medium- and long-term future.

The 'National Cyber Security Framework Manual' is intended to provide both academics and policy-makers with an in-depth examination of the relevant factors when dealing with cyber security within a national security context. The theoretical frameworks employed are intended to help further understanding of the various facets of the issue, not to prescribe a certain political or developmental path. Indeed, national cyber security as a topic is sufficiently complex that no one individual approach can be seen as being universally valid across all nations and all local circumstances. Like the very term itself, each interpretation of 'cyber security' is contingent on the position – and purpose – of the observer.

Alexander Klimburg
Vienna, Austria

September 2012

# 1. PRELIMINARY CONSIDERATIONS: ON NATIONAL CYBER SECURITY

*Melissa E. Hathaway, Alexander Klimburg*

## 1.1. INTRODUCTION

What, exactly, is 'national cyber security'? There is little question that the advent of the internet is having a decisive influence on how national security is being defined. Nations are increasingly facing the twin tensions of how to expedite the economic benefits of ICT[1] and the internet-based economy while at the same time protecting intellectual property, securing critical infrastructure and providing for national security. Most nations' electronic defences have been punctured and the potential costs of these activities are considerable. More than one hundred nations have some type of governmental cyber capability and at least fifty of them have published some form of a cyber strategy defining what security means to their future national and economic security initiatives.[2] There can be little doubt, therefore, that countries have an urgent need to address cyber security on a national level. The question is how this need is being formulated and addressed.

This section provides a context for how national cyber security can be conceived. It provides an introduction, not only to the topic itself, but also to the Manual as a whole, setting the scene for the further sections to explore in depth. Accordingly, this section highlights the broad set of terms and missions being used to describe the overall cyber environment. It examines how various nations integrate their respective concepts of national security and cyber security, and proposes its own definition of what national cyber security could entail. Three conceptual tools are introduced to help focus the strategic context and debate. These are termed the 'three dimensions', the 'five mandates', and the 'five dilemmas' of national cyber security. As the reader will discover, each dimension, mandate and dilemma will play a varying role in each nation's attempt to formulate and execute a national cyber security strategy according to their specific conditions. This section, like the Manual as a whole, does not attempt to prescribe a specific set of tasks or a checklist of issues that need to be resolved. Rather, it concentrates on helping to formulate a conceptual picture of what 'national cyber security' can entail.

---

1 'Information and communications technology' used interchangeably with the term 'information technology' (IT).

2 James A. Lewis and Katrina Timlin, Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization, (Geneva: UNIDIR, 2011), http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

### 1.1.1. Cyber: Converging Dependencies

The internet, together with the information communications technology (ICT) that underpins it, is a critical national resource for governments, a vital part of national infrastructures, and a key driver of socio-economic growth and development. Over the last forty years, and especially since the year 2000, governments and businesses have embraced the internet, and ICT's potential to generate income and employment, provide access to business and information, enable e-learning, and facilitate government activities. In some countries the internet contributes up to 8% of gross domestic product (GDP), and member countries of both the European Union (EU) and the G20 have established goals to increase the internet's contribution to GDP.[3] This cyber environment's value and potential is nurtured by private and public sector investments in high-speed broadband networks and affordable mobile internet access, and break-through innovations in computing power, smart power grids, cloud computing, industrial automation networks, intelligent transport systems, electronic banking, and mobile e-commerce.

The rise of the internet, and the increasing social dependence on it, did not occur overnight. The first 'internet' transmission occurred in October 1969 with a simple message between two universities. Now, 294 billion e-mail are sent per day. Internet protocols evolved during the 1970s to allow for file sharing and information exchange. Now, in one day, enough information is generated and consumed to fill 168 million DVDs. In 1983 there was a successful demonstration of the Domain Name System (DNS) that provided the foundation for the massive expansion, popularisation and commercialisation of the internet. E-commerce and the e-economy were made possible in 1985 with the introduction of top-level-domains (e.g., .mil, .com, .edu, .gov) and this growth was further fuelled in 1990 with the invention of the world wide web which facilitated user-friendly information sharing and search services. Today, nearly two-thirds of the internet-using population research products and businesses online before engaging with them offline, and most use search engines like Google, Baidu, Yahoo, and Bing to complete that research. Social networks now reach over 20% of the global population.[4] SMS traffic generates $812,000 every minute.[5]

---

3 David Dean et al., 'The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy,' *BCG. Perspectives*, 27 January 2012.

4 comScore, 'It's a Social World: Top 10 Need-to-Knows About Social Networking and Where It's Headed,'http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/it_is_a_social_world_top_10_need-to-knows_about_social_networking.

5 ITU-D, The World in 2010. ICT Fact and Figures, (Geneva: ITU, 2010), http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

In 1996, the International Telecommunications Union (ITU) adopted a protocol that allowed transmission of voice communication over a variety of networks. This innovation gave way to additional technological breakthroughs like videoconferencing and collaboration over IP networks. Today, 22 million hours of television and movies are watched on Netflix and approximately 864,000 hours of video are uploaded to YouTube per day.[6] Skype has over 31 million accounts and the average Skype conversation lasts 27 minutes.[7] The mobile market has also exploded, penetrating over 85% of the global population. 15% of the population use their mobile phones to shop online and there are now more mobile phones on the planet than there are people.[8]

The internet economy has delivered economic growth at unprecedented scale, fuelled by direct and ubiquitous communications infrastructures reaching almost anyone, anywhere. At the same time, infrastructure modernisation efforts have embraced the cost savings and efficiency opportunities of ICT and the global reach of the internet. Over the past decade, businesses replaced older equipment with cheaper, faster, more ubiquitous hardware and software that can communicate with the internet. At the heart of many of these critical infrastructures is an industrial control system (ICS) that monitors processes and controls the flow of information. Its functionality is like the on or off feature of a light switch. For example, an ICS can adjust the flow of natural gas to a power generation facility, or the flow of electricity from the grid to a home. Over the last decade, industry has increased connections to and between critical infrastructures and their control system networks to reduce costs and increase efficiency of systems, sometimes at the expense of resiliency.[9]

Today, businesses around the world tender services and products through the internet to more than 2.5 billion citizens using secure protocols and electronic payments. Services range from e-government, e-banking, e-health and e-learning to next generation power grids, air traffic control and other essential services, all of which depend on a single infrastructure.[10] The economic, technological, political and social benefits of the internet are at risk, however, if it is not secure, protected and available. Therefore, the availability, integrity and resilience of this core infrastructure have emerged as national priorities for all nations.

---

6 Cara Pring, '100 Social Media, Mobile and Internet Statistics for 2012 (March),' *The Social Skinny*, 21 March 2012.

7 Statistic Brain, 'Skype Statistics,' *Statistic Brain*, 28 March 2012.

8 Edward Coram-James and Tom Skinner, 'Most Amazing Internet Statistics 2012,' Funny Junk, http://www.funnyjunk.com/channel/science/Most+Amazing+Internet+Statistics+2012/umiNGhz.

9 Melissa E. Hathaway, 'Leadership and Responsibility for Cybersecurity,' *Georgetown Journal of International Affairs* Special Issue (Forthcoming).

10 Services and applications include, but are not limited to: e-mail and text messaging, voice-over-IP-based applications, streaming video and real-time video-conferencing, social networking, e-government, e-banking, e-health, e-learning, mapping, search capabilities, e-books, and IPTV over the internet.

It is anticipated that a decade from now, the internet will touch 60% of the world's population (over 5 billion citizens); will interlink more than 50 billion physical objects and devices; and will contribute at least 10% of developing nations' GDP including China, Brazil, India, Nigeria and the Russian Federation.[11] These predictions, if realised, will certainly alter politics, economics, social interaction and national security. How countries nurture and protect this infrastructure will vary. Hard choices and subtle tensions will have to be reconciled, because there are at least two competing requirements under constrained fiscal budgets: delivering economic wellbeing and meeting the security needs of the nation.

**Table 2:** Today and the Near Future[12]

| | Today | 2020 |
|---|---|---|
| **Estimated World Population** | 7 billion people | ~8 billion people |
| **Estimated Internet Population** | 2.5 billion people (35% of population is online) | ~5 billion people (60% of population is online) |
| **Total Number of Devices** | 12.5 billion internet connected physical objects and devices (~6 devices per person) | 50 billion internet connected physical objects and devices (~10 devices per person) |
| **ICT Contribution to the Economy** | ~4% of GDP on average for G20 nations | 10% of worldwide GDP (and perhaps more for developing nations) |

## 1.1.2. The Cost of Connectivity

Governments around the world are pushing for citizen access to fast, reliable, and affordable communications to meet the demand curve of the e-economy. This vision is reflected in the Organisation for Economic Co-operation and Development's (OECD) Internet Economy; Europe's Digital Agenda; the United States' National Broadband Plan, and in most ITU initiatives. A number of developing nations have grasped the importance of ICT for development. Brazil, for instance, is in the middle of a major upgrade to its broadband infrastructure.[13] Progress towards becoming

---

11 Dave Evans, The Internet of Things. How the Next Evolution of the Internet Is Changing Everything, (San Jose, CA: Cisco Internet Business Solutions Group, 2011), http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

12 Evans, *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything.*

13 Angelica Mari, 'IT's Brazil: The National Broadband Plan' *itdecs.com*, 26 July 2011.

an advanced member of the information society is often measured in terms of lower price-points, expanded bandwidth, increased speed and better quality of service, expanded education and developed skills, increased access to content and language, and targeted applications for low-end users.[14] But is the ITU measuring the right things? Should the ITU also be measuring the attendant investments in the security of that infrastructure, connectivity and information service? For example, South Korea was ranked the most advanced nation in the ITU's information society in terms of its internet penetration, high-speed broadband connections and ICT usage; yet it was also ranked by the Internet security research firm Team Cymru as 'Asia-Pacific's leading host of peer-to-peer botnets.'[15] South Korea is not the only advanced nation to experience the challenges of connectivity. Highly-connected countries are tempting targets for criminals.[16] In fact, according to Symantec, the G20 nations harbour the majority of malicious code and infected computers. Among the top three countries are China, Germany, and the United States; of those three, the United States accounts for the highest number (23%) of all malicious computer activity.[17]

The internet is under siege and the volume, velocity, variety, and complexity of the threats to the internet and globally connected infrastructures are steadily increasing. For example, it is estimated that the G20 economies have lost 2.5 million jobs to counterfeiting and piracy, and that governments and consumers lose $125 billion annually, including losses in tax revenue.[18] Organisations everywhere are being penetrated, from small businesses to the world's largest institutions. Criminals have shown that they can harness bits and bytes with precision to deliver spam, cast phishing attacks, facilitate click-fraud and launch distributed denial of service (DDoS) attacks.[19] Attack toolkits sold in the underground economy for as little as $40 allow criminals to create new malware and assemble an entire attack plan

---

14 ITU, Measuring the Information Society, (Geneva: ITU, 2011), http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf. See also Melissa E. Hathaway and John E. Savage, Stewardship of Cyberspace. Duties for Internet Service Providers, (Cambridge, MA: Belfer Center for Science and International Affairs, 2012), http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012_hathaway-savage.pdf.

15 Botnet: compromised, internet-connected computers typically used for illegal activities, usually without the owner's knowledge.

16 Reuters, 'South Korea discovers downside of high speed internet and real-name postings,' *The Guardian*, 6 December 2011.

17 Ibid.

18 Frontier Economics Europe, Estimating the global economic and social impacts of counterfeiting and piracy. A Report commissioned by Business Action to counterfeiting and piracy (BASCAP), (Paris: ICCWBO, 2011), http://www.iccwbo.org/Data/Documents/Bascap/Global-Impacts-Study---Full-Report.

19 See Melissa E. Hathaway, 'Falling Prey to Cybercrime: Implications for Business and the Economy,' in *Securing Cyberspace: A New Domain for National Security*, ed. Nicholas Burns and Jonathon Price (Queenstown, MD: Aspen Institute, 2012).

without having to be a software programmer.[20] In 2011, Symantec identified over 400 million unique variants of malware that exposed and potentially exfiltrated personal, confidential, and proprietary data.[21] Many governments suffered data breaches in 2011, including Australia, Brazil, Canada, India, France, New Zealand, Russia, South Korea, Spain, Turkey, the Netherlands, the United Kingdom and the United States. Hundreds of companies have also suffered significant breaches in 2011-2012, including Citigroup, e-Harmony, Epsilon, Linked-In, the Nasdaq, Sony and Yahoo. One industry report estimates that over 175 million records were breached and another industry report estimates that it cost enterprises £79 ($125.55) per lost record,[22] excluding any fines that may have been imposed for violations of national data privacy laws.

At the same time, the pace of foreign economic collection and industrial espionage activities against major corporations and governments is also accelerating. The hyper-connectivity and relative anonymity provided by ICT lowers the risk of being caught and makes espionage straightforward and attractive to conduct. In recent testimony before the United States Congress, the Assistant Director of the Counterintelligence Division of the FBI told lawmakers that the FBI is 'investigating economic espionage cases responsible for $13 billion in losses to the US economy.'[23] Some of the cases referenced include the targeting, penetration, and compromising of companies that produce security products. In particular, certificate authorities including Comodo, DigiNotar, and RSA, fell prey to their own weak security postures, which were subsequently exploited facilitating a wave of other computer breaches.[24] Digital certificates represent a second form of identity to help enhance 'trust' for financial or other private internet transactions by confirming that something or someone is genuine.[25] These certificates have become the *de facto* credentials used for secure online communications and sensitive transactions, such as online banking or accessing corporate e-mail from a home computer.

---

20 Symantec Corporation, Internet Security Threat Report: 2011 Trends, (Mountain View, CA: Symantec Corporation, 2012), http://www.symantec.com/threatreport.

21 Ibid., 9.

22 Verizon, 2012 Data Breach Investigations Report, (Arlington, VA: Verizon Business, 2012), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf; Ponemon Institute, 2010 Annual Study: U.K. Cost of a Data Breach. Compliance pressures, cyber attacks targeting sensitive data drive leading IT organisations to sometimes pay more than necessary, (Mountain View, CA: Symantec Corporation, 2011), http://www.symantec.com/content/en/us/about/media/pdfs/UK_Ponemon_CODB_2010_031611.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach.

23 U.S. House of Representatives, *Testimony: Before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives: Committee on Homeland Security*, 28 June 2012.

24 Hathaway, 'Leadership and Responsibility for Cybersecurity.'

25 Certificate Authorities issue secure socket layer (SSL) certificates that help encrypt and authenticate websites and other online services.

During oral testimony before the US Senate Armed Services Committee, US Army General Keith Alexander identified China as the prime suspect behind the RSA penetration and subsequent theft of intellectual property.[26] Perhaps the US National Counter-Intelligence Executive put it best when he reported that, '[m]any states view economic espionage as an essential tool in achieving national security and economic prosperity. Their economic espionage programs combine collection of open source information, HUMINT, signals intelligence (SIGINT), and cyber operations – to include computer network intrusions and exploitation of insider access to corporate and proprietary networks – to develop information that could give these states a competitive edge over the United States and other rivals.'[27]

Finally, unauthorised access, manipulation of data and networks, and destruction of critical resources also threatens the integrity and resilience of critical core infrastructures. The proliferation and replication of worms like Stuxnet, Flame, and Duqu that can penetrate and establish control over remote systems is alarming. In an April 2012 newsletter, the Industrial Control System Computer Emergency Readiness Team (ICS-CERT) disclosed that it was investigating attempted intrusions into what it described as 'multiple natural gas pipeline sector organisations.' It went on to say that the analysis of the malware and artefacts associated with this activity was related to a single campaign with the initial penetration, resulting from spear-phishing multiple personnel.[28] While the Stuxnet attack against Iran was quite sophisticated, it does not necessarily require a strong industrial base or a well-financed operation to find ICS vulnerabilities – teenagers regularly are able to accomplish the task.[29] Those motivated to do harm seek software vulnerabilities – effectively errors in existing software code – and create malware to exploit them, subsequently compromising the integrity, availability and confidentiality of the ICT networks and systems.[30] Some researchers hunt for these 'zero-day' vulnerabilities on behalf of governments, others on behalf of criminal syndicates, but many 'white hat' researchers constantly do the same job for little or no pay. To encourage the 'white hat' security community to effectively find holes in their commercial

---

26 U.S. Senate Committee on Armed Services, *Statement of General Keith B. Alexander, Commander United States Cyber Command*, 27 March 2012.

27 U.S. Office of the National Counterintelligence Executive, Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, (Washington, DC: US Office of the National Counterintelligence Executive, 2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

28 ICS-CERT, ICS-CERT Monthly Monitor, (Washington, DC: US Department of Homeland Security, 2012), http://www.us-cert.gov/control_syssupratems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf.

29 Robert O'Harrow, 'Cyber search engine Shodan exposes industrial control systems to new risks,' *The Washington Post*, 3 June 2012.

30 Hathaway, 'Leadership and Responsibility for Cybersecurity.'

products before criminals or cyber warriors do, companies like Google, Facebook, and Microsoft have programmes that pay for responsibly disclosed vulnerabilities.[31]

The above examples illustrate that the internet and its associated global networks have greatly increased the world's dependence on ICT and thus also increased the level of disruption that is possible when the infrastructure is under attack. And it is constantly under attack, both by state and non-state actors. Although the problem is obvious, the role of government *vis-à-vis* the private sector in the protection of this critical infrastructure is often still unclear. This lack of clarity and vision regarding government action is not totally unsurprising, however. To date, there is not even a universal understanding on basic cyber terms and definitions, so common solutions will remain scarce.

## 1.2. CYBER TERMS AND DEFINITIONS

The internet, the ICT that underpin it and the networks that it connects are at times also referred to as comprising 'cyberspace'. Merriam-Webster defines 'cyber' as: 'of, relating to, or involving computers or computer networks (as the Internet).'[32] Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks. The ITU uses the term to describe the 'systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks.'[33] The International Organisation for Standardisation (ISO) uses a slightly different term, defining cyber as 'the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.'[34] Separately, governments are defining what they mean by cyberspace in their national cyber security strategies (NCSS). For example, in its 2009 strategy paper, the United Kingdom refers to cyberspace as 'all forms of networked, digital activities; this includes the content of and actions conducted through digital networks.'[35] By adding the phrase, 'the content of and actions conducted through,' the government

---

31 Chris Rodriguez, 'Vulnerability Bounty Hunters,' *Frost & Sullivan*, 3 February 2012.

32 Cyber, Merriam-Webster, http://www.merriam-webster.com/dictionary/cyber.

33 ITU, ITU National Cybersecurity Strategy Guide, (Geneva: ITU, 2011), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf. 5.

34 ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity.'

35 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space* (Norwich: The Stationery Office, 2009). 7. However, in 2011 a new definition of cyberspace was put forward understood as an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services (see UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (London: UK Cabinet Office, 2011).).

can also address human behaviours that it finds acceptable or objectionable. For some nations, this includes consideration of internet censorship, online information control, freedom of speech and expression, respect for property, protection of individual privacy, and the protection from crime, espionage, terrorism, and warfare. Governments, businesses, and citizens know intuitively that cyberspace is man-made and an ever-expanding environment, and that therefore the definitions are also constantly changing.

### 1.2.1. Information, ICT, and Cyber Security

Most governments start their NCSS process by describing the importance of 'securing information', implementing 'computer security' or articulating the need for 'information assurance'. These terms are often used interchangeably, and contain common core tenets of protecting and preserving the confidentiality, integrity and availability of information. 'Information security' focuses on data regardless of the form the data may take: electronic, print or other forms. 'Computer security' usually seeks to ensure the availability and correct operation of a computer system without concern for the information stored or processed by the computer. 'Information assurance' is a superset of information security, and deals with the underlying principles of assessing what information should be protected. Effectively, all three terms are often used interchangeably, even if they address slightly different viewpoints. Most unauthorised actions that impact any of the core tenets or information security attributes[36] are considered a crime in most nations.

The globalisation of the ICT marketplace and increasing reliance upon globally sourced ICT products and services can expose systems and networks to exploitation through counterfeit, malicious or untrustworthy ICT. And while not defined in diplomatic fora, the term 'ICT security' is often used to describe this concern. In general, ICT security is more directly associated with the technical origins of computer security, and is directly related to 'information security principles' including the confidentiality, integrity and availability of information resident on a particular computer system.[37] ICT security, therefore, extends beyond devices that are connected to the internet to include computer systems that are not connected to any internet. At the same time, the use of the term 'ICT security' usually excludes all questions of illegal content, unless they directly damage the system in question, and includes the term 'supply chain security'.

---

36 The most basic attributes are Confidentiality, Integrity and Availability, and are known as the C-I-A triad. Some systems expand this by including authenticity, reliability, or any number of other attributes as well.

37 See, for instance, US DoC/NIST, Minimum Security Requirements for Federal Information and Information Systems, (Gaithersburg, MD: NIST, 2006), http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

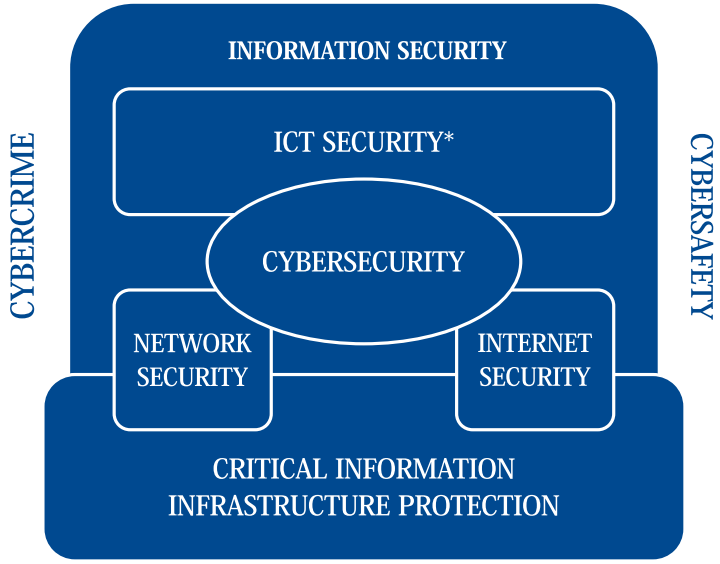


**Figure 1:** Relationship between Cyber Security and other Security Domains[38]

[38] This Figure has been adopted from ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity.' It slightly differs from the original in that it contains ICT Security* instead of 'Application Security'. The latter has been defined as 'a process to apply controls and measurements to an organization's applications in order to manage the risk of using them. Controls and measurements may be applied to the application itself (its processes, components, software and results), to its data (configuration data, user data, organization data), and to all technology processes and actors involved in the application's life circle' (ibid., 10.). Information Security 'is concerned with the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user' (ibid.). Network Security 'is concerned with the design, implementation, and operation of networks for achieving the purposes of information security on networks within organizations, between organizations, and between organizations and users' (ibid.). Internet Security 'is concerned with protecting internet-related services and related ICT systems and networks as an extension of network security in organizations and at home, to achieve the purpose of security. Internet Security also ensures the availability and reliability of Internet services' (ibid., 11.). CIIP 'is concerned with protecting the systems that are provided or operated by critical infrastructure providers, such as energy, telecommunication, and water departments. CIIP ensures that those systems and networks are protected and resilient against information security risks, network security risks, internet security risks, as well as Cybersecurity risks' (ibid.). Cybercrime has been defined as the 'criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime' (ibid., 4.). Cybersafety has been defined as the 'condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable' (ibid.). 'Cybersecurity', or 'Cyberspace Security' has been defined as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace' (ibid.). However, it has also been noted that '[i]n addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved' (ibid.) in cyber security.

The United States, India, Russia and many other countries are increasingly voicing concerns that the introduction of counterfeit, malicious or untrustworthy ICT could disrupt the performance of sensitive national security systems, and compromise essential government services. The ICT supply chain consists of many phases, including design, manufacture, integrate, distribute, install and operate, maintain and decommission. The processes by which nations consider the security of their ICT supply chain should try to address each phase of the lifecycle. Protection measures must be developed across the product lifecycle and be reinforced through both acquisition processes and effective implementation of government/enterprise security practices. For example, the highest risk factors in the supply chain are 'after build' (e.g., during the install and operate and retire phases) because this is where multiple vendors participate in the process (e.g., integrate products with other systems, patch/update, etc.) and there are few measures to monitor and assure integrity throughout the entire process. This is a problem for all countries: the evolution of the ICT industry means that many countries and global corporations now play a role in the ICT supply chain, and no country can source all components from totally 'trusted providers'. This trust is needed, however, as the promise of ICT-driven economic growth is dependent upon the core infrastructure being both secure and resilient.

There is no agreed definition of 'internet security'. Within a technical context, internet security 'is concerned with protecting internet-related services and related ICT systems and networks as an extension of network security in organizations and at home, to achieve the purpose of security. Internet security also ensures the availability and reliability of internet services.'[39] However, in a political context, internet security is often equated with what is also known as 'internet safety'. In general, internet safety refers to 'legal internet content'. While this has sometimes been linked to government censorship in autocratic governments, restrictions on internet content are, in fact, common. Besides issues surrounding the exploitation of children, internet censorship can also include issues such as intellectual property rights as well as the prosecution of political or religious views. What internet security probably does not include is non-internet relevant technical issues, including those that address the various 'internets' which are not connected to the world wide web. These, however, are covered by the term 'network security'. Network security is particularly important for critical infrastructures that are often not directly connected to the internet. Consequently, for some, internet security implies a global government regime to deal with the stability of the internet code and hardware, as well as the agreements on the prosecution of illegal content.

39 ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity,' 11.

The term 'cyber security' was widely adopted during the year 2000 with the 'clean-up' of the millennium software bug.[40] When the term 'cyber security' is used, it usually extends beyond information security and ICT security. ISO defined cyber security as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace.'[41] The Netherlands defined cyber security more broadly, to mean 'freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information.'[42] The ITU also defined cyber security broadly as:

> '[T]he collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.'[43]

Many countries are defining what they mean by cyber security in their respective national strategy documents. As of the publication of this Manual, more than 50 nations have published some form of a cyber strategy defining what security means to their future national and economic security initiatives.

When the term 'defence' is paired with 'cyber' it usually is within a military context, but also may take into account criminal or espionage considerations. For example, the North Atlantic Treaty Organisation (NATO) uses at least two terms when it comes to cyber defence and information security. The first addresses a broader information security environment: communications and information systems[44]

---

40 The millennium bug was a problem for both digital (computer-related) and non-digital documentation and data storage situations which resulted from the practice of abbreviating a four-digit year to two digits.

41 ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity.'

42 Dutch Ministry of Security and Justice, 'The National Cyber Security Strategy (NCSS). Strength through Cooperation,' (The Hague: National Coordinator for Counterterrorism and Security, 2011), 4.

43 Recommendation ITU-T X.1205 (04/2008), Section 3.2.5.

44 CIS security is defined as: The ability to adequately protect the confidentiality, integrity, and availability of Communication and Information Systems (CIS) and the information processed, stored or transmitted.

(CIS) security, where 'security' is defined as the ability to adequately protect the confidentiality, integrity and availability of CIS and the information processed, stored or transmitted.[45] NATO uses a different definition for the term 'cyber defence': 'the ability to safeguard the delivery and management of services in an operational CIS in response to potential and imminent as well as actual malicious actions that originate in cyberspace.'[46] The United States military defines it in two contexts as well. The first, from the Joint Staff, defines 'computer network defence' (CND) as: 'actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.'[47] Finally, the newly formed United States Cyber Command operationalised the term and defines 'defensive cyber operations' as: 'direct and synchronize actions to detect, analyse, counter and mitigate cyber threats and vulnerabilities; to outmanoeuvre adversaries taking or about to take offensive actions; and to otherwise protect critical missions that enable US freedom of action in cyberspace.'[48]

The common theme from all of these varying definitions, however, is that cyber security is fundamental to both protecting government secrets and enabling national defence, in addition to protecting the critical infrastructures that permeate and drive the 21st century global economy. The slight differentiation in definition between governments and intergovernment organisations is irrelevant, as their shared focus on the issues illustrates the first step in the long journey to actually providing for cyber security – no matter what the definition.

### 1.2.2. Cyber Crime

There does not appear to be a common view regarding what constitutes illegal or illicit activity on the internet. Yet most would agree that one of the fastest-growing areas of crime is that which is taking place in cyberspace.[49] Efforts to clarify and address this issue began in the United Nations (UN) in 1990, where the General Assembly (UN GA) debated and adopted a resolution dealing with computer crime legislation which was later expanded in 2000 and again in 2002 to combat the

45 Geir Hallingstad and Luc Dandurand, *Cyber Defence Capability Framework – Revision 2. Reference Document RD-3060* (The Hague: NATO C3 Agency, 2010).

46 Ibid.

47 US Joint Chiefs of Staff, Joint Publication 6-0. Joint Communications System, (Ft. Belvoir, VA: DTIC, 2010), http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

48 GAO, Defense Department Cyber Efforts. More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities, (Washington, DC: GAO, 2011), http://www.gao.gov/products/GAO-11-421. 5.

49 Europol, Threat Assessment (Abridged). Internet Facilitated Organised Crime (iOCTA), (The Hague: Europol, 2011), https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf.

criminal misuse of ICT.[50] As a result, these early discussions encouraged countries to update their penal codes. For example, in 1997, the Russian government updated the Russian Penal Code (Chapter 28) to address cyber crime, IT crime, and cyber terrorism. Penalties were identified for, among other things, illegal access to the information on a computer, computer systems and networks; creation, spreading and usage of harmful software and malware; violation of operation instructions of a computer, computer systems and networks; illegal circulation of objects of intellectual property; illegal circulation of radio-electronic and special high-tech devices; and manufacturing and spreading of child pornography.

Also in 1997, the felonies of 'illegal intrusion into a computer information system' and 'causing damage to a computer information system' were specifically added to the Criminal Law of the People's Republic of China. In June 2010, the Information Office of the State Council published a white paper on the internet in China. It detailed China's principles for the internet and identified particular activities that were objectionable to the state. For example, it stated: 'the security of telecommunications networks and information shall be protected by law. No organization or individual may utilise telecommunication networks to engage in activities that jeopardise state security, the public interest or the legitimate rights and interests of other people.'[51] In addition to China and Russia, many other countries also have updated their legal frameworks to address criminal activities in accordance with the spirit of the discussion that began nearly 25 years ago.

The Council of Europe (CoE) also adopted a Convention on Cybercrime in July 2004,[52] the first international convention to address this issue. It contains a relatively high standard of international cooperation for investigating and prosecuting cyber crime. It recognised that criminals exploit the seams of cross-jurisdictional cooperation and coordination among nations. The treaty defined key terms such as 'computer system', 'computer data', 'traffic data', and 'service provider' in an effort to create commonality among signatories' existing statutes, but does not define the key term 'cybercrime'. The treaty went on to highlight actions that nations must undertake to prevent, investigate and prosecute, including copyright infringement, computer-related fraud, child pornography and violations of network security. For example, it outlined offences against the confidentiality, integrity and availability of computer data and systems (e.g., illegal access, illegal interception, data interference, system interference, misuse of devices). It also discussed computer-related fraud and forgery. The treaty also contained a series of powers and procedures, such as the

50 Marco Gercke, 'Regional and International Trends in Information Society Issues,' in *HIPCAR – Working Group 1* (St. Lucia: ITU, 2010).

51 Chinese Information Office of the State Council, *The Internet in China (White Paper)* (Beijing: Government of the People's Republic of China, 2010).

52 Council of Europe, *Convention on Cybercrime (ETS No. 185)* (Budapest: Council of Europe, 2001).

search of computer networks and interception. Over ten years after the treaty was formed, it has been signed by 47 states, and has been ratified by 37.[53, 54] This is controversial in some nations, and might explain the relatively small number of countries that have managed to approve the treaty in accordance with their domestic constitutional requirements and thereby making it enforceable.

Other organisations have taken similar approaches, within their own frameworks. In July 2006, the ASEAN Regional Forum (ARF) issued a statement that its members should implement cyber crime and cyber security laws 'in accordance with their national conditions and should collaborate in addressing criminal and terrorist misuse of the Internet.'[55] These commitments were later codified in the 2009 agreement within the Shanghai Cooperation Organization (ASEAN-China Framework Agreement) on information security. Additionally, it is the only international treaty that addresses concerns of a wider concept of 'information war', which the treaty defined as 'confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, and undermining political, economic and social systems, mass brainwashing to destabilise society and state, as well as forcing the state to take decisions in the interest of an opposing party.'[56]

Illicit and illegal activity definitions differ from region to region. Online fraud, online theft and other forms of cyber crimes which misappropriate the property of others are on the rise. It is inexpensive to develop and use malware, as was observed in 2011 with the 400 million unique variants and as many as eight new zero-day vulnerabilities were exploited per day.[57] As citizens adopt and embed more mobile devices into their business and personal lives, it is likely that malware authors will create mobile specific malware geared toward the unique opportunities that the mobile environment presents for abuse of electronic transactions and payments. Nations around the world have identified cyber crime (however it is defined) as a national priority. They also recognise that jurisdiction for prosecuting cyber crime stops at national borders, which underscores the need for cooperation and coordination through regional organisations like ASEAN and the Council of Europe.

---

53 Brian Harley, 'A Global Convention on Cybercrime?,' *Science and Technology Law Review*, 23 March 2010.

54 Council of Europe, 'Convention on Cybercrime (Treaty Status),' http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

55 Greg Austin, 'China's Cybersecurity and Pre-emptive Cyber War,' *NewEurope*, 14 March 2011.

56 See Shanghai Cooperation Organization, *Agreement on Cooperation in the Field of Ensuring International Information Security [based on unofficial translation]* (Yekaterinburg: Shanghai Cooperation Organization, 2009). Annex I; Nils Melzer, 'Cyber operations and *jus in bello*,' *Disarmament Forum*, no. 4 (2011).

57 Symantec Corporation, *Internet Security Threat Report: 2011 Trends*. See also Hathaway, 'Falling Prey to Cybercrime: Implications for Business and the Economy.'

### 1.2.3. Cyber Espionage

Cyberspace provides an exceptional environment for espionage because it provides 'foreign collectors with relative anonymity, facilitates the transfer of a vast amount of information, and makes it more difficult for victims and governments to assign blame by masking geographic locations.'[58] While some nations define these intrusions or unauthorised access to data or an automated information system as an 'attack,' most of the observed activity today does not qualify as an attack under international law. It is considered to be theft of commercial intellectual property and proprietary information, of data with significant economic value, or the theft of government sensitive and classified information. These given considerations are defined by almost all nations as criminal acts first, and espionage second. This is also a simple necessity: with the rise of presumed state-sponsored industrial espionage, it is very often unclear if an activity that for certain can be categorised as cyber crime should instead be described as cyber espionage.

Espionage is defined as, 'the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company.'[59] In this context, espionage is when foreign governments or criminal networks steal information or counterfeit goods in ways that erode the public's trust in internet services. It is pervasive throughout the world, the number of businesses falling victim to these crimes increases daily and no sector is without compromise. Companies and governments regularly face attempts by others to gain unauthorised access through the internet to their data and information technology systems by, for example, masquerading as authorised users or through the surreptitious introduction of malicious software.[60] Some define this activity as Computer Network Exploitation (CNE): enabling operations and intelligence collection capabilities through the use of computer networks to gather data from target or adversary automated information systems or networks.[61] It is important to note that CNE is often an enabling prerequisite for disruptive or damaging activities on an information system (see below).

However it is defined, cyber espionage, particularly when targeting commercial intellectual property, risks, over time, undermining a national economy. Many countries use espionage to spur rapid economic growth based on advanced technology, targeting science and technology initiatives of other nations. Because

---

58 US Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011.*

59 Espionage, Merriam-Webster, http://www.merriam-webster.com/dictionary/espionage.

60 See Hathaway, 'Falling Prey to Cybercrime: Implications for Business and the Economy.'

61 U.S. Joint Chiefs of Staff, Joint Publication 3-13. Information Operations, (Ft. Belvoir, VA: DTIC, 2006), http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

ICT forms the backbone of nearly every other technology used in both civilian and military applications today, it has become one of the primary espionage targets. Of course, military and civilian dual-use technologies will remain of interest to foreign collectors, especially advanced manufacturing technologies that can boost industrial competitiveness.

### 1.2.4. 'Cyber Warfare'

The term 'cyber warfare' is both ambiguous and controversial – there is no official or generally accepted definition. While the term itself is virtually never used in official documents, its relatives – 'Information Operations' (Info Ops or also IO) and 'Information Warfare' (IW) – are commonly used, albeit with different meanings. More than 30 countries have an articulated doctrine and have announced dedicated offensive cyber warfare programmes, mostly using IO or IW as terminology.[62] Nonetheless, the term 'cyber war' has a useful academic purpose, in terms that it concentrates thinking on state to state conflict within and through cyberspace, and the ramifications this can have. Accordingly, cyber warfare has become an unavoidable element in any discussion of international security. For example, Russia discusses information warfare methods as a means to 'attack an adversary's centres of gravity and critical vulnerabilities,' and goes on to state that by doing so, 'it is possible to win against an opponent, militarily as well as politically, at a low cost without necessarily occupying the territory of the enemy.'[63, 64] This doctrine is a synthesis of the official position of state policy for maintaining information security. Likewise, China also discusses information warfare in depth, and the need to conduct offensive operations exploiting the vulnerabilities and dependence of nations on ICT and the internet in a recently published book.[65] China continues

---

62 Lewis and Timlin, *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization.*

63 Roland Heickerö, Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations, (Stockholm: Swedish Defence Research Agency 2010), http://www.highseclabs.com/Corporate/foir2970.pdf. 18.

64 Alexander Klimburg and Heli Tirmaa-Klaar, Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU, (Brussels: European Parliament, 2011), http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf.

65 For a recent non-state Chinese account see Hunan People's Publishing House, *China Cyber Warfare: We Can't Lose the Cyber War* (Hunan: China South Publishing & Media Group).

to evolve its military strategy and doctrine for conducting information warfare campaigns and taking advantage of the 'informationisation'[66] of society.

Of course when nations begin to discuss cyber warfare, they need to clarify what they mean by cyber attack.[67] Germany defines a cyber attack as an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security – confidentiality, integrity and availability – which may all or individually be compromised.[68] The United Kingdom outlined four different methods of cyber attack in its national cyber strategy: electronic attack, subversion of supply chain, manipulation of radio spectrum, disruption of unprotected electronics using high power radio frequency.[69] The United States defines Computer Network Attack (CNA) as 'actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'.[70] The difference between the US and German definition of cyber attack is an illustrative one: the US definition does not include attacks on confidentiality (e.g., through a 'probe' or espionage) as a cyber attack while, according to the German definition, there is no difference between a probe and a cyber attack. The term takes on different meanings to meet the security remit of different communities. For example, it is natural for the military to be ambiguous as to whether an attack is considered a use of force (as defined by the Law of Armed Conflict), whereas the law enforcement community (police and prosecutors) are more likely to describe an attack as a crime. Incident response professional and technical experts will likely use the term to generically characterise any malicious attempt against confidentiality or availability. A single definition will not help this, but clarity about which meaning of 'attack' is meant in a particular context can help reduce confusion.

In general, there is agreement that cyber activities can be a legitimate military activity, but there is no global agreement on the rules that should apply to it. This is further complicated by the ambiguous relationship between cyber war and cyber

---

66 China has is promoting informationisation development for economic restructuring, infrastructure modernisation, and national security. It is similar to the Digital Agenda of Europe, in that it is promoting all the means to accelerate the process from the industry society to the information society. It contains seven areas of emphasis: (1) ICT and ICT industries (manufacture, service); (2) ICT applications (e-gov, e-commerce); (3) Information Resources (Content); (4) Information Infrastructure (Network); (5) Information Security; (6) Talents (all kinds); (7) Laws, Regulations, Standards, and Specifications (see Xiaofan Zhao, 'Practice and Strategy of Informatization in China,' (Shanghai: UPAN, 2006).).

67 See Section 3.1.3 for a more detailed examination of cyber attack classifications.

68 German Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011). 14-5.

69 UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*: 13-4.

70 U.S. Joint Chiefs of Staff, *Joint Publication 3-13. Information Operations*.

espionage – there is a very fine line between breaking into a computer to spy and breaking in to attack.[71] Nations are concerned that infrastructure disruption could inflict significant economic costs on the public and private sectors and impair performance of essential services. This is why some nations are demanding a dialogue regarding what constitutes a legitimate target in cyberspace, code of conduct for stewardship and conflict, and the need for confidence building measures to reduce the risk of unwanted or unnecessary miscalculation and subsequent escalation of conflict and misunderstanding.

For example, China, Russia, Tajikistan and Uzbekistan introduced an International Code of Conduct for Information Security for consideration by the 66th UN General Assembly.[72] This document was intended to jumpstart discussion on wide-ranging approaches for dealing with appropriate behaviours in cyberspace. This specific proposal and the overall concept of a 'code of conduct', will likely be raised at a number of upcoming international fora dealing with cyber security and internet policy matters.

To date, it appears that the United States and a number of European countries oppose the notion that a code of conduct or treaty is needed to address cyber warfare. They argue that the proposed obligations seem to be in conflict with existing international law built around concepts such as refraining from the 'threat or use of force' (Article 2(4) of the UN Charter) and the right to exercise 'self-defence if an armed attack occurs' (Article 51 of the UN Charter). Moreover, it is unclear how a proposed code's concepts of 'hostile activities' and 'threats to international peace and security' relate to the 'threat or use of force' standard in Article 2(4), or whether the proposed code would constrain the inherent right to self-defence recognised in Article 51. Other nations are taking the initiative to drive debate and resolution regarding what is needed, given the economic and national security consequences of what is at stake. These efforts have taken on a new tempo and seriousness given the use of Stuxnet against Iran's nuclear infrastructure. For example, the United Kingdom hosted a conference on norms of behaviour in London in 2011 to help foster an international dialogue, and it is expected that this discussion will continue in Hungary and South Korea in the coming years.

---

71 James Lewis, 'Confidence-building and international agreement in cybersecurity,' *Disarmament Forum*, no. 4 (2011): 56.

72 See UNGA, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)* (New York: United Nations, 2011).

## 1.3. NATIONAL CYBER SECURITY

There is no universally accepted explicit definition of what constitutes 'national cyber security' (or NCS for short). Indeed, although the exact term is hardly ever used in official strategies, it is commonly employed by government spokespersons without ever being defined. NCS has two obvious roots: the term 'cyber security' and the term 'national security' – both of which are often differently defined in official national documents. Even if the term 'national cyber security' is seldom explicitly defined, it is possible to derive a working definition based on the respective use of the other two terms.

### 1.3.1. Comparison of 'National' and 'Cyber' Security

When analysing the use of the terms 'cyber security' and 'national security' in official documents, it is first and foremost necessary to accept that national differences (to say nothing of linguistic differences) will often prevent a direct and literal comparison. As discussed above, the term 'cyber security' does not have a single accepted common definition, and this is especially the case when used within public policy documents. Also, the term 'national security' is not always defined even within a specific national context – an often intentional move aimed to provide government with needed flexibility.[73]

Until relatively recently, the term 'national security' was largely used only within the United States. The widespread introduction of dedicated 'national security strategies' (NSS) in a number of OECD countries is a relatively recent phenomenon that appears to have been closely tied to a shift in strategic thought away from focusing on a few specific 'threats' to the idea against of mitigation against myriad 'risks'. Thus, for example, in nearly all of the post-2007 strategies, cyber security is defined as a key national security issue. Indeed, in some cases, the topic of 'cyber security' (or even 'national cyber security') predates the actual creation of the national security strategy, and sometimes even seems to function as a driver for the paradigm shift to a more comprehensive national security strategy; one in which the state not only recognises that various risks need to be addressed, but that they only can be addressed by working together with non-state actors.

---

73 For example, the UK Security Service (also known as MI5) states that: 'The term 'national security' is not specifically defined by UK or European law. It has been the policy of successive Governments and the practice of Parliament not to define the term, in order to retain the flexibility necessary to ensure that the use of the term can adapt to changing circumstances' (UK Security Service (MI5), 'Protecting National Security,' https://www.mi5.gov.uk/home/about-us/what-we-do/protecting-national-security.html.).

When looking at specific countries, this paradigm shift becomes fairly clear. Australia, for instance, published its First National Security Statement to its Parliament in 2008,[74] which was put in place as part of a long-term reform agenda to establish a sustainable national security policy framework. When the Australian government released its Cyber Security Strategy[75] in 2009, it was clear that the strategy dealt with both Australia's national security and its digital economy. While the National Security Strategy highlights the vitality of 'partnerships between industry, governments and the community',[76] in order to maintain 'a secure, resilient and trusted electronic operating environment',[77] the government's cyber security policy has a similar emphasis on partnerships with the private sector; while simultaneously referring to the fact that 'the Australian Government has an important leadership role'.[78]

Although the term 'national security' has been used in Canada since the 1970s, the first official incorporation of a national security strategy did not occur until 2004.[79] However, as set out in its National Security Strategy, threats that 'undermine the security of the state of society [...] generally require a national response, as they are beyond the capacity of individuals, communities or provinces to address alone.'[80] In context with Canada's cyber security strategy, this implies 'a shared responsibility, one in which Canadians, their governments, the private sector and our international partners all have a role to play.'[81]

In Germany, at least until 2008, the term '*Sicherheitspolitik*' was considered to be sufficiently analogous to the English term 'national security'. But in recent years the term 'national security' has taken root in German policy and political discourse, perhaps in an effort to draw attention to the increased blurring of national and international risks (as opposed to the threat-based model of the Cold War) requiring an increased 'national' cooperation. As part of these efforts, the term 'cyber security' might be considered directly analogous to 'national cyber security', in that it is also directly tied with a single specific programme – the national protection plan for the critical information infrastructure.[82]

---

74 Australian Prime Minister, *The First National Security Statement to the Australian Parliament* (Canberra: Australian Government, 2008).

75 Australian Attorney-General's Department, *Cyber Security Strategy* (Canberra: Australian Government, 2009).

76 Ibid., 5.

77 Ibid.

78 Ibid.

79 Canadian Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Canadian Government, 2004).

80 Ibid., vii.

81 Canadian Department for Public Safety, *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada* (Ottawa: Canadian Government, 2010). 17.

82 The implementation of this protection plan is known as UP-KRITIS (civilian) and UP-BUND (for government).

Similarly, in France there was no formal tradition of the term 'national security' until 2008, when it was first introduced in the Defence White Book.[83] In contrast to Germany, the concept of national security was comprehensively defined, based upon both 'defence' (military) and 'domestic' (internal) civilian strategies, together with an overall set of guiding principles.[84] Recent French government documents[85] make it clear that 'cyber defence' aims to protect the security of France's 'critical information systems' according to 'information assurance measures'.

The first British National Security Strategy was introduced in 2008 and has been reviewed at least two times since. The rationale for moving away from the previous emphasis on Strategic Defence Reviews or Defence White Papers was made quite clear:

> 'The aim of this first National Security Strategy is to set out how we will address and manage this diverse though interconnected set of security challenges and underlying drivers, both immediately and in the longer term, to safeguard the nation, its citizens, our prosperity and our way of life.'[86]

The focus on this 'diverse set of security challenges' was particularly directed at cyber security. To enjoy freedom and prosperity in cyberspace, the government set out four guiding objectives: successful handling of cyber crime; establishing the UK as one of the most secure places in the world to do business; improvement of resilience to cyber attacks, and protection of national interests in cyberspace.[87] The British National Cyber Strategy is a comprehensive document that goes beyond national security issues. Although the 'national security' component of the Cyber Security Strategy remains partially classified, it appears to be well funded in that over £650 million was made available for the period 2011-2015. Interestingly, the definition of cyber security seems equally concerned with protecting systems as well as 'exploiting opportunities' and encompasses missions as diverse as internet governance, trade policy, counter-terrorism and intelligence.

---

83 French White Paper Commission, *The French White Paper on Defence and National Security* (Paris: Odile Jacob, 2008).

84 'The 'republican compact' that binds all French people to the State, namely the principles of democracy, and in particular individual and collective freedoms, respect for human dignity, solidarity and justice' (ibid., 58.).

85 French Secretariat-General for National Defence and Security, *Information systems defence and security. France's strategy* (Paris: French Network and Information Security Agency, 2011).

86 UK Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world* (Norwich: The Stationery Office, 2008).

87 UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*: 21.

## Table 3: National (Cyber) Security Strategies in Selected OECD Countries

| | NATIONAL SECURITY | | | CYBER SECURITY | | | NATIONAL CYBER SECURITY |
|---|---|---|---|---|---|---|---|
| | Document | Year | Basic Definition / Understanding | Document | Year | Basic Definition / Understanding | Key Objectives / Areas |
| AU | The First National Security Statement to the Parliament[88] | 2008 | 'Freedom from attack or the threat of attack; the maintenance of our territorial integrity; the maintenance of our political sovereignty; the preservation of our hard won freedoms; and the maintenance of our fundamental capacity to advance economic prosperity for all Australians.' | Cyber Security Strategy[89] | 2009 | 'Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.' | Three key objectives:<br>- 'All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online'<br>- 'Australian Businesses operate secure and resilient informations and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers'<br>- 'The Australian Government ensures its information and communications technologies are secure and resilient' |
| CA | Securing an Open Society: Canada's National Security Policy[90] | 2004 | 'National security deals with threats that have the potential to undermine the security of the state or society. These threats generally require a national response, as they are beyond the capacity of individuals, communities or provinces to address alone.<br>National security is closely linked to both personal and international security. While most criminal offences, for example, may threaten personal security, they do not generally have the same capacity to undermine the security of the state or society as do activities such as terrorism or some forms of organized crime.<br>Given the international nature of many of the threats affecting Canadians, national security also intersects with international security. At the same time, there are a growing number of international security threats that impact directly on Canadian security and are addressed in this strategy.' | Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada[91] | 2010 | 'detect, identify and recover' from cyber attacks which 'include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security.' | Three pillars:<br>- 'Securing Government systems'<br>- 'Partnering to secure vital cyber systems outside the federal Government'<br>- 'Helping the Canadians to be secure online' |

88 Australian Prime Minister, *The First National Security Statement to the Australian Parliament.*

89 Australian Attorney-General's Department, *Cyber Security Strategy.*

90 Canadian Privy Council Office, *Securing an Open Society: Canada's National Security Policy.*

91 Canadian Department for Public Safety, Canada's Cyber Security Strategy. *For a Stronger and More Prosperous Canada.*

92 Federal Ministry of Defence, *White Paper 2006 on German Security Policy and the Future of the Bundeswehr* (Berlin: Federal Ministry of Defence, 2006).

93 German Federal Ministry of the Interior, *Cyber Security Strategy for Germany.*

94 French White Paper Commission, *The French White Paper on Defence and National Security.*

95 French Secretariat-General for National Defence and Security, *Information systems defence and security. France's strategy.*

96 Dutch Government, *Strategie Nationale Veiligheid* (The Hague: Ministry of the Interior and Kingdom Relations, 2007).

97 Dutch Ministry of Security and Justice, 'The National Cyber Security Strategy (NCSS). Strength through Cooperation.'

98 UK Cabinet Office, *The National Security Strategy: A Strong Britain in an Age of Uncertainty* (Norwich: The Stationary Office, 2010).

99 UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.*

100 White House, *National Security Strategy* (Washington, DC: White House, 2010).

101 White House, *The National Strategy to Secure Cyberspace.*

102 *National Security Presidential Directive 54: Cyber Security and Monitoring (NSPD-54) / Homeland Security Presidential Directive 23: Cyber Security and Monitoring (HSPD-23).*

103 Public Safety and Homeland Security Bureau, 'Tech Topic 20: Cyber Security and Communications,' FCC, http://transition.fcc.gov/pshs/techtopics/techtopics20.html.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **DE** | White Paper 2006 on German Security Policy and the Future of the Bundeswehr[92] | 2006 | 'German security policy is based on a comprehensive concept of security; it is forward-looking and multilateral. Security cannot be guaranteed by the efforts of any one nation or by armed forces alone. Instead, it requires an all-encompassing approach that can only be developed in networked security structures.' | Cyber Security Strategy for Germany[93] | 2011 | 'Cyber security and civilian and military cyber security: (Global) cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures. Civilian cyber security focuses on all IT systems for civilian use in German cyberspace. Military cyber security focuses on all IT systems for military use in German cyberspace.' | Ten strategic areas (objectives and measures):<br>- 'Protection of critical information infrastructures'<br>- 'Secure IT systems in Germany'<br>- 'Strengthening IT security in the public administration'<br>- 'National Cyber Response Centre'<br>- 'National Cyber Security Council' | - 'Effective crime control also in cyberspace'<br>- 'Effective coordinated action to ensure cyber security in Europe and worldwide'<br>- 'Use of reliable and trustworthy information technology'<br>- 'Personnel development in federal authorities'<br>- 'Tools to respond to cyber attacks' |
| **FR** | The French White Paper on Defence and National Security[94] | 2008 | 'The aim of France's National Security strategy is to ward off risks or threats liable to harm the life of the nation. Its first aim is to defend the population and French territory, this being the first duty and responsibility of the State. The second aim is to enable France to contribute to European and international security: this corresponds both to its own security needs, which also extend beyond its frontiers, and to the responsibilities shouldered by France within the framework of the United Nations and the alliances and treaties which it has signed. The third aim is to defend the values of the 'republican compact' that binds all French people to the State, namely the principles of democracy, and in particular individual and collective freedoms, respect for human dignity, solidarity and justice.' | Information systems defence and security: France's strategy[95] | 2011 | 'The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence.' | Four strategic objectives:<br>'- Become a cyberdefence world power in cyberdefence<br>- Safeguard France's ability to make decisions through the protection of information related to its sovereignty<br>- Strengthen the cybersecurity of critical national infrastructures<br>- Ensure security in cyberspace' | |
| **NL** | Strategie Nationale Veiligheid[96] | 2007 | [*Own Translation*] 'National security is at stake when the vital interests of our state and/or our society [1. territorial security, 2. economic security, 3. ecological security, 4. physical security, and 5. social and political security] are threatened in such way that it leads to – potential – social disruption. National security contains both the corrosion of security by intentional human action (security) as well as the damage caused by disasters, system or process failures, human error or natural anomalies such as extreme weather (safety).' | The National Cyber Security Strategy (NCSS): Strength through cooperation[97] | 2011 | 'Cyber security is freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information.' | 'Security and trust in an open and free digital society:<br>The Strategy's goal is to strengthen the security of digital society in order to give individuals, businesses, and public bodies more confidence in the use of ICT. To this end, the responsible public bodies will work more effectively with other parties to ensure the safety and reliability of an open and free digital society.<br>This will stimulate the economy and increase prosperity and well-being. It will ensure legal protection in the digital domain, prevent social disruption, and lead to appropriate action if things go wrong.' | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **UK** | A Strong Britain in an Age of Uncertainty: The National Security Strategy[98] | 2010 | 'The security of our nation is the first duty of government. It is the foundation of our freedom and our prosperity.' [...] 'The National Security Strategy of the United Kingdom is: to use all our national capabilities to build Britain's prosperity, extend our nation's influence in the world and strengthen our security.' | The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world[99] | 2011 | actions taken 'to reduce the risk and secure the benefits of a trusted digital environment for businesses and individuals.' | Four objectives:<br>'- The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace<br>- The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace<br>- The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societie<br>- The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives' | |
| **US** | National Security Strategy[100] | 2010 | 'Our national security depends upon America's ability to leverage our unique national attributes, just as global security depends upon strong and responsible American leadership. That includes our military might, economic competitiveness, moral leadership, global engagement, and efforts to shape an international system that serves the mutual interests of nations and peoples. For the world has changed at an extraordinary pace, and the United States must adapt to advance ou interests and sustain our leadership.' | The National Strategy to Secure Cyberspace[101] | 2003 | 'protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible. Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector, and the American people.' | Three Strategic Objectives:<br>'- Prevent cyber attacks against America's critical infrastructures<br>- Reduce national vulnerability to cyber attacks; and<br>- Minimize damage and recovery time from cyber attacks that do occur.' | |
| | | | | National Security Presidential Directive 4[102] (partially unclassified)[103] | 2008 | [*From the 2009 Cyberspace Policy Review*]<br><br>'cybersecurity policy [...] includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure.' | [*From the 2008 National Security Presidential Directive 54*]<br><br>Thirteen Objectives:<br>'- establishing the National Cyber Security Center within the Department of Homeland Security'<br>'- Move towards managing a single federal enterprise network;<br>- Deploy intrinsic detection systems;<br>- Develop and deploy intrusion prevention tools;<br>- Review and potentially redirect research and funding;<br>- Connect current government cyber operations centers; | - Develop a government-wide cyber intelligence plan;<br>- Increase the security of classified networks;<br>- Expand cyber education;<br>- Define enduring leap-ahead technologies;<br>- Define enduring deterrent technologies and programs;<br>- Develop multi-pronged approaches to supply chain risk management; and<br>- Define the role of cyber security in private sector domains.' |
| | | | | Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure | 2009 | | | |

The Netherlands was one of the first countries to move away from a threat-based national security picture to a more 'risk' based view.[104] As part of this shift, the first Dutch National Security Strategy was adopted in 2007, with a detailed work plan leading to the eventual adoption of a national cyber security strategy in 2011. The drafting of the strategy was coordinated by the Ministry of Security and Justice, and was a response to the Parliament's demand (referred to as the Amendment Knops) for the creation of a 'National Cyber Strategy'. The document was conceived as providing a road-map to a Whole of Government approach to national security.[105] The definition of national security is closely aligned to the philosophy of 'Comprehensive Security'[106] and initiated a national risk assessment based approach to decision making.[107] The language within the NCSS is clearly orientated toward 'ICT-based threats', and the Dutch definition of cyber security contemplates the 'freedom from danger or damage due to the disruption, breakdown, or misuse of ICT.'

The United States has used the term 'national security' at least since 1947, and in the ensuing six decades, the implicit meaning of 'national security' has changed many times – an explicit meaning was often avoided in order to secure an advantage through strategic ambiguity.[108] Since 1986, the United States has produced 15 National Security Strategies (NSS), the most recent of which was published in 2012. The US definition of 'national security' is much wider than commonly employed abroad. While 'securing cyberspace' is also a particular item within the NSS 2010, the majority of mentions of 'cyber' are outside of that particular section, illustrating that the issue is considered to be cross-vertical and not, in the most narrow sense, a security issue alone. Similarly, the US has avoided creating a dedicated single overarching national cyber security strategy, instead relying on a collection of documents to fulfil the same goal. Since the White House first established formal

---

104 For an in-depth study, see Michel Rademaker, 'National Security Strategy of the Netherlands: An Innovative Approach, '*Information and Security* 23, no. 1 (2008), http://infosec.procon.bg/v23/Rademaker.pdf.

105 See, for instance, Marcel de Haas, From Defence Doctrine to National Security Strategy: The Case of the Netherlands, (The Hague: Netherlands Institute of International Relations Clingendael, 2007), http://www.clingendael.nl/publications/2007/20071100_cscp_art_srsa_haas.pdf.

106 The five securities are *Territorial*, *Economic*, *Physical*, *Ecological* and *Social/Political*.

107 Dutch Ministry of Security and Justice, 'The National Cyber Security Strategy (NCSS). Strength through Cooperation.'

108 According to a US defence department manual, 'national security' is '[a] collective term encompassing both national defence and foreign relations of the United States. Specifically, the condition provided by: a. a military or defence advantage over any foreign nation or group of nations; b. a favourable foreign relations position; or c. a defence posture capable of successfully resisting hostile or destructive action from within or without, overt or covert' (U.S. Joint Chiefs of Staff, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, (Ft. Belvoir, VA: DTIC, 2012), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.).

structures in 1998 to coordinate various cyber security activities,[109] a number of documents have been released that can claim to directly address strategic national cyber security issues.[110] Yet there is no clear definition of what the US government considers to be cyber security, although the term 'national cyber security' (albeit undefined) has been employed.[111]

## 1.3.2. Cyber Power and National Security

Until fairly recently there have been few theoretical models of interstate conflict and international relations that directly have cyber security at their core. The concept of 'cyber warfare' is highly contentious, not the least because, for liberal democratic governments, the distinction between warfare and mere attacks is a vital one. Not all approaches, however, make the distinction between peacetime and wartime activities. The purported Chinese 'Information Warfare'[112] concept (known as 'Three Warfares') includes methods such as 'Legal Warfare' and 'Media Warfare' that might seem to be anathema to liberal democracies, yet certainly acknowledges the importance of information in the so-called Information Age. While some nations cannot easily countenance such strategies, it is clear that a new conflict paradigm is necessary, one that acknowledges the importance of the information domain while not violating hallowed principles of democracy. An equally important question is how to include the breadth of national cyber security issues and functions in times of both peace and war, and across the different components of 'national power',[113] e.g., to exert 'cyber power'.

---

109 The Critical Infrastructure Protection (PDD-63) as part of: *National Security Presidential Directive 54: Cyber Security and Monitoring (NSPD-54) / Homeland Security Presidential Directive 23: Cyber Security and Monitoring (HSPD-23).*

110 These include: White House, *The National Strategy to Secure Cyberspace* (Washington, DC: White House, 2003); *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7)*; White House, *The Comprehensive National Cybersecurity Initiative (as codified in NSPD-54/HSPD-23)* (Washington, DC: White House, 2008); White House, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: White House, 2009); White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (Washington, DC 2011).

111 The context is a Whole of Government Cyber Security Strategy and, in particular, enhanced cooperation between the Department of Homeland Security and the Department of Defense. Overall, the term 'national cyber security' implies here the protection of the .mil and .gov domain, and the ability of the systems within these domains to operate normally at home and abroad (US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC 2011). 8.).

112 For a comprehensive study of the 'Three Warfares Study' see Timothy Walton, 'Treble Spyglass, Treble Spear?: China's Three Warfares,' *Defense Concepts* 4, no. 4 (2009).

113 Concepts of 'national power' refer to leverages of power of a nation-state or alliance; and can include different specific instruments. Most commonly these are referred to as including Diplomatic, Military, Informational and Economic (DIME) instruments. These are active in times of peace and war.

What actually constitutes power in and through cyberspace within the larger framework of national power is still poorly understood and the subject of much debate. What is clear is that the 'cyber power' of a nation does not necessarily derive solely from the amount of trained hackers it has, but rather the sum total of resources or capabilities it can leverage to pursue political and economic goals while ensuring the resilience of its own infrastructure.

One attempt to define cyber power reads: 'the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.'[114] This definition illustrates what has become official policy not only in the United States, but also in many countries in Europe: cyberspace is viewed as an operational domain of military operations, equal to land, air, sea and space.[115] Unlike the other domains of conflict, however, cyberspace plays a role across each of the 'instruments of national power'. Each of these instruments is therefore directly influenced by cyber means.[116]

This approach to cyber security and national power has one particular disadvantage – it is very much a 'major power' doctrine, most applicable to nations whose size or intent propels them to seek a highly proactive engagement in the international strategic landscapes, i.e., to actively 'create strategic opportunities via cyberspace'. The discourse has largely emerged from the military, despite other attempts to define cyber power within a 'soft power' context.[117] Not all nations will share these goals of power projection.

The concept of 'national cyber security' that is seemingly emerging by default, rather than by intent, addresses a more modest set of requirements than notions of cyber power. While military capabilities and international power-projection still play a role, the view is often more orientated towards managing the cyber risks that a nation faces, rather than proactively trying to exploit those cyber risks in advancing its global power. Nations that seek to define a pronounced NCSS often do so more with a view towards domestic security, rather than expanding their global

---

114 Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyber Power and National Security* (Washington, DC: National Defence UP, 2009).Kramer and his colleagues, however, approach the issue primarily from a military perspective. A slightly broader view was offered by Joseph Nye, who considers the most important application of soft (cyber) power to be outward-facing, influencing nations, rather than inward-facing (see Joseph S. Nye, Cyber Power, (Cambridge, MA: Belfer Center for Science and International Affairs, 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.).
See Mark Thompson, 'U.S. Cyberwar Strategy: The Pentagon Plans to Attack,' *Time*, 2 February 2010.

115 See, for instance, US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*.

116 Kramer, Starr, and Wentz, *Cyber Power and National Security*.

117 Nye, *Cyber Power*; Alexander Klimburg, 'The Whole of Nation in Cyberpower,' *Georgetown Journal of International Affairs* Special Issue (2011).

strategic position. Accordingly, for the purposes of this Manual, we will define 'national cyber security' as:

> 'the focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security.'

## 1.4. CONCEPTUALISING NATIONAL CYBER SECURITY

As discussed above, what ultimately constitutes national cyber security (NCS) will always remain in the eye of the beholder. However, any overall strategy that seeks to address NCS will most likely need to orientate itself according to various parameters: what is the purpose of the strategy? who is the intended audience? These questions will be addressed in full in Section 2 as they are standard questions for any national security strategy, and are independent of the cyber security domain. What is inherent to the cyber security topic are more specific questions: firstly, where is the strategy directed at, what is its actual purpose, who are the stakeholders? This question is addressed in more depth in Section 3. Secondly, how is the cyber security domain segmented, and how are the different interpretations of NCS understood? This question is addressed in more depth in Section 4. And thirdly, how does this all relate to the wider well-being of the nation?

For these last three questions this Manual suggests three conceptual tools to help focus strategic deliberations: respectively, they are termed the 'three dimensions', the 'five mandates', and the 'five dilemmas' of national cyber security. Together they provide for a comprehensive view of the topic. Not all NCSS will want to provide equal weight to the different aspects of national cyber security described in this Manual. Therefore, these tools are intended to provide an overview of what aspects can be considered, rather than a checklist of what should be taken into account.

### 1.4.1. The Three Dimensions: Governmental, National and International[118]

Any approach to a NCS strategy needs to consider the 'three dimensions' of activity: the governmental, the national (or societal) and the international. Since the 1990s a particular trend in public policy theory has focused on the cooperation of different

[118] See Section 3 for further details. Based on Klimburg, 'The Whole of Nation in Cyberpower.'

actors. Initially the focus was on improving the coordination of government actors (the Whole of Government approach or WoG), particularly between the departments most involved in stabilisation or peace building operations in places like Afghanistan or Iraq. Subsequently, the general notion was picked up by international organisations as diverse as NATO and the International Committee of the Red Cross, who backed concepts of international, trans-border and 'like for like' collaboration (also called the Whole of System approach or WoS) rather than intergovernmental cooperation. More recently, states have begun looking at better methods for cooperating with their 'national' non-state actors, ranging from aid and humanitarian groups to critical infrastructure providers (sometimes called the Whole of Nation approach or WoN) or even, more generally, their national civil society.

The lessons learned from the prolonged engagements in countries like Afghanistan and Iraq emphasise the importance and the challenge of different actors working together. The same challenges apply even more so to the field of national cyber security where, if anything, power and responsibility is distributed far more widely than within so-called stabilisation or peace building operations.

**Governmental:** within government alone, it is not unusual for up to a dozen different departments and agencies to claim responsibility for national cyber security in various forms, including military, law enforcement, judicial, commerce, infrastructure, interior, intelligence, telecommunications, and other governmental bodies. This is understandable due to breadth and depth of what constitutes NCS but leads to considerable difficulty in establishing coherent action. A major challenge for all NCS strategies is, therefore, improving the coordination between these governmental actors. This Whole of Government effort can be achieved by a number of different methods, ranging from appointing a lead agency or department to simply improving the inter-departmental process. Due to the esoteric nature of cyber security, however, it probably requires much more effort to achieve this Whole of Government synergy than practically any other security challenge.

**International:** virtually no NCS document ignores the international dimension. The very basis of the internet,[119] to say nothing of the myriad companies and organisations that effectively constitute the internet, is thoroughly globalised. For any nation state or interest group, to advance its interests requires collaboration with a wide range of international partners. This applies at any level: from internationally binding treaties (e.g., the Council of Europe Cybercrime Convention), to politically binding agreements (e.g., regarding Confidence Building Measures

[119] The internet is marked by the routing of data 'packets' and these packets rarely take the most direct geographic route: it is perfectly possible for an e-mail sent from Los Angeles to New York to be routed through China and Russia on the way.

in Cyberspace), to non-governmental agreements between technical certification bodies (e.g., membership of FIRST[120] and similar bodies). Many of the international collaborations will occur outside a specific national government. In fact, it can be necessary to work with non-state actors abroad. Therefore, the emphasis must be on relationships with all the relevant actors within specific systems (in particular, but not limited to the field of 'internet governance'). This Whole of System approach, therefore, emphasises the need for a government to agree on a single lead actor (which can be also outside of government itself), and to enable that actor to be flexible enough to engage with the entire range of actors globally.[121]

**National:** engagement with security contractors and critical infrastructure companies has always been seen as critical for national security. The steady expansion of the number of actors relevant to national cyber security within any particular nation has meant that some governments have decided to make their overall strategy 'comprehensive', including the entire society, or the Whole of Nation. A Whole of Nation approach tries to overcome the limitations of simply having special legally-defined relationships with a small number of specific security contractors. Often it tries to encourage a wide range of non-state actors (in particular private companies but also research establishments and civil society) to cooperate with the government on cyber security issues. While many governments are increasingly expanding their legal options, the general principle is that specific 'cooperation' is needed from such a great number of non-state actors that a pure legislative approach would be largely unworkable in most democracies. To encourage cooperation, Whole of Nation approaches usually include various incentives that directly support the security of these enterprises, and indirectly can be of other advantage as well (e.g., commercially).

### 1.4.2. The Five Mandates of National Cyber Security[122]

Within the general context of discussing national cyber security, it is important to keep in mind that this is not one single subject area. Rather, it is possible to split the issue of NCS into five distinct perspectives or 'mandates', each of which could be addressed by different government departments. This split is not an ideal state

---

120 The 'Forum of Incident Response and Security Teams' (FIRST) is an international certification organisation for Computer Emergency Response Teams (CERTs, sometimes CSIRTs). CERTs are the principle organisation form for dealing with all manner of technical cyber security tasks and national CERTs that wish to belong to FIRST must be certified by the organisation.

121 As an example, the US government interaction with part of worldwide technical CERT community is largely managed by the non-governmental Carnegie-Mellon University.

122 See Section 4.3 for additional details. Based on Klimburg in Alexander Klimburg and Philipp Mirtl, Cyberspace and Governance – A Primer (Working Paper 65), (Vienna: Austrian Institute for International Affairs, 2012), http://www.oiip.ac.at/publikationen/arbeitspapiere/publikationen-detail/article/92/cyberspace-and-governance-a-primer.html.

but it is a reality due to the complexity and depth of cyber security as a whole. Each mandate has developed its own emphasis and even its own lexicon, despite the fact that they are all simply different facets of the same problem. Unfortunately, there is frequently a significant lack of coordination between these mandates, and this lack of coordination is perhaps one of the most serious organisational challenges within the domain of national cyber security.

**Military Cyber:** the internet security company McAfee has been warning since 2007 that, in its opinion, a 'virtual arms race' is occurring in cyberspace with a number of countries deploying cyber weapons.[123] Many governments are building capabilities to wage cyber war,[124] while some NATO reports have claimed that up to 120 countries are developing a military cyber capability.[125] These capabilities can be interpreted as simply one more tool of warfare, similar to airpower, which would be used only within a clearly defined tactical military mission (for instance, for shutting down an air-defence system). Military cyber activities, therefore, encompass four different tasks: enabling protection of their own defence networks, enabling Network Centric Warfare (NCW) capabilities, battlefield or tactical cyber warfare, and strategic cyber warfare.

**Counter Cyber Crime:** cyber crime activities can include a wide swathe of activities that impact both the individual citizen directly (e.g., identity theft) and corporations (e.g., theft of intellectual property). At least as significant for national security, however, is the logistical support capability cyber crime can offer to anyone interested in conducting cyber attacks. This is also where cyber crime interacts not only with military cyber activities, but also with cyber terrorism. As of 2012, there has not occurred any event that would be considered a 'cyber terrorist' attack despite, for instance, threats by the hacker group Anonymous to 'bring down the internet.'[126] This said, there have been a rising number of criminal acts, including attempts at mass disruption of communications, and this suggests cyber terrorism will be an issue for the future.

**Intelligence and Counter-Intelligence:** distinguishing cyber espionage from cyber crime and military cyber activities is controversial. In fact, both missions depend on similar vectors of attack and similar technology. In practice, however, serious espionage cases (regarding intellectual property as well as government secrets) are in a class of their own, while at the same time it can be very difficult to ascertain for sure if the perpetrator is a state or a criminal group operating on behalf of a

123 See Zeenews, 'US, China, Russia have 'cyber weapons': McAfee,' *Zeenews.com*, 18 November 2009.

124 See Michael W. Cheek, 'What is Cyber War Anyway? A Conversation with Jeff Carr, Author of 'Inside Cyber Warfare',' *The new new Internet*, 2 March 2010.

125 See Julian Hale, 'NATO Official: Cyber Attack Systems Proliferating,' *DefenceNews*, 23 March 2010.

126 Tyler Holman, 'Anonymous threatens to bring down the internet,' *Neowin.net*, 27 March 2012.

state, or indeed operating on its own. Whoever is actually behind the attack, cyber espionage probably represents the most damaging part of cyber crime (if included in the category). Cyber espionage, when directed toward states, also makes it necessary to develop specific foreign policy response mechanisms capable of dealing with the inherent ambiguity of actor-nature in cyberspace. At the same time, counter-intelligence activities (i.e., detecting and combating the most sophisticated cyber intrusions) very often will depend upon other types of intelligence activity, including human intelligence, signals intelligence, forensic analysis, etc., as well as extensive information sharing between international partners.

**Critical Infrastructure Protection and National Crisis Management:** critical infrastructure protection (CIP) has become the catch-all term that seeks to involve the providers of essential services of a country within a national security framework. As most of the service providers (such as public utilities, finance or telecommunications) are in the private sector, it is necessary to extend some sort of government support to help protect them and the essential services they provide from modern threats. While the original focus of these programmes post-September 11, 2001 was often on physical security, today the majority of all CIP activity is directly connected to cyber acts, usually cyber crime and cyber espionage. In this context, National Crisis Management must be extended by an additional cyber component. This includes institutional structures which enhance the cooperation between state and non-state actors both nationally and internationally, as well as a stable crisis communication network and an applicable legal framework to exchange relevant information.[127]

**'Cyber Diplomacy' and Internet Governance:** if diplomacy at its core is about how states exchange, deal with, gather, assess, present and represent information,[128] cyber diplomacy is about 'how diplomacy is adapting to the new global information order.'[129] Within this context, the promotion of aims such as 'norms and standards for cyber behaviour' (discussed primarily within the UN) and the aim for promoting 'confidence building measures between nations in cyberspace' needs to be understood as a mostly bilaterally-focused activity. Internet governance, in contrast, is largely a multilateral (or even multi-stakeholder) activity, and is probably the most international of all mandates. Internet governance is generally referred to as

---

127 See, for instance, Austrian Federal Chancellery, *National ICT Security Strategy Austria* (Vienna: Digital Austria, 2012). 14-5.

128 Adapted from Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (Basingstoke: Macmillan, 1977). 170-83.

129 Evan H. Potter, ed. *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century* (Quebec: McGill-Queen's University Press, 2002), 7. Potter originally is discussing 'e-diplomacy', which however in this Manual is defined as the ability to conduct diplomacy with cyber means.

the process by which a number of state and non-state actors interact to manage what, in effect, is the programming (or code, or 'logical') layer of the internet.

The above segmentation is an attempt to provide for a more structured discussion on the scope of national cyber security. The reality of these different mandates is that they are each dealt with by different organisational groups not only within government, but also within the non-state sector. Normatively speaking, all of these mandates should be holistically engaged if a comprehensive NCS perspective is to be developed.

## 1.5. THE FIVE DILEMMAS OF NATIONAL CYBER SECURITY

National cyber security is a tool to reach a desired state of affairs, not an end in itself. Most nations define a strategic goal of a safe and secure environment within which they can achieve full economic potential, and protect citizens from various cyber and non-cyber related risks, both domestic and foreign. To achieve this, NCS has to deal with its own, overarching set of 'national cyber security dilemmas'. In international relations theory, the traditional 'security dilemma' states that both a country's security strength and its weakness can create unfavourable reactions in their adversaries.[130] The NCS Dilemmas are, however, different: both a strong and a weak NCS posture can have economic and social costs.

### 1.5.1. Stimulate the Economy vs. Improve National Security

Nations are constantly facing the twin tensions of how to expedite the economic benefits of ICT and the internet economy while, at the same time, protecting intellectual property and privacy (data protection), securing critical infrastructure, and providing for defence of the homeland. The productivity promise that ICT brings for some nations will approach 10% of their GDP by 2015.[131] This growth is being documented in policies and funded through initiatives around the world. For example, the European Union is pursuing the Digital Agenda, the United States is pursuing the Innovation Agenda, and China is pursuing a policy of

---

[130] See, for instance, Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976). 66-72.

[131] Soumitra Dutta and Irene Mia, The Global Information Technology Report 2009-2010. ICT for Sustainability, (Geneva: World Economic Forum, 2010), http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf. 12 and 61. See also Scott C. Beardsley et al., 'Fostering the Economic and Social Benefits of ICT,' *The Global Information Technology Report 2009-2010* (Geneva: World Economic Forum, 2010), http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf; Dean et al., 'The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy.'

'Informationisation'. The agendas have common components: provision of high-speed internet to citizens and businesses modernisation of critical infrastructures with new ICT components that can communicate with the internet and promotion of research and innovation to ensure that innovative ideas can be turned into products and services that create growth and jobs and, ultimately, drive competitiveness. Businesses and governments embrace the efficiency savings that ICT presents and are accelerating the pace and mechanisms by which transactions and services are conducted over the internet. Businesses are using just-in-time manufacturing and retail distribution, and essential services like electricity, water, and fuel supply are increasingly being managed over the internet. ICT is the platform for innovation, prosperity and advancing a nation's economic and national security interests.

The success of a nation's ability to leverage ICT to achieve the desired economic stimulus and social benefits should depend on its use of the different market levers to assure the confidentiality, integrity and availability, and the security of networks and information systems that are central to the economy and society. The most important issue, however, remains, simply put, cost – it supersedes all other concerns, including those of security. This is certainly short-sighted: the advances of ICT can be more than off-set through ICT-amplified disasters. The security of the ICT hardware supply chain, for example, is a well-known issue but an issue where there are seemingly no simple and, most importantly, no cheap solutions.[132]

Despite increasing awareness of the associated risks, consumers and large businesses do not take advantage of available technology and processes to secure their systems, nor do they take protective measures to blunt the evolving threat. This general lack of investment puts firms and consumers at greater risk, leading to economic loss at the individual and aggregate level and thus poses direct a threat to national security.[133] Three issues are central to the national security debate: how does the government assure the availability of essential services; provide for the protection of intellectual property; and maintain citizen confidence (and safety) when participating in the internet economy? Nations are struggling with finding the appropriate mix of policy interventions and market levers to boost the impacts of ICT. Connectivity among individuals, businesses and markets demand more robust security to reduce consumer risk and enable organisations to offer better service and increased capabilities online. Policy intervention (both regulatory and

---

[132] One programme intended to provide 'trusted' microchips for sensitive US ICT systems is the 'Trusted Foundry Program' (Catherine Ortiz, 'DOD Trusted Foundry Program: Ensuring 'Trust' for National Security & Defense Systems,' in *NDIA Systems Engineering Division Meeting* (Arlington, VA: Trusted Foundry Program, 2012).).

[133] US Department of Commerce, Cybersecurity, Innovation, and the Internet Economy (Green Paper), (Gaithersburg, MD: NIST, 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

incentives based) must harness the capabilities and responsibilities of the private sector to achieve a prudent level of security without hindering productivity, trade or economic growth.

### 1.5.2. Infrastructure Modernisation vs. Critical Infrastructure Protection

A key tension that stems from the economic vs. national security debate is the tension between the forces that are driving infrastructure modernisation (economic stimulus) *vis-à-vis* the forces that are demanding critical infrastructure protection.[134] These infrastructures are being modernised, harnessing affordable access to broadband applications and services, and inexpensive ICT devices. As such, they increasingly comprise a heterogeneous composite of hardware and software products that, for the most part, combine unverified hardware and software that is manufactured by a heterogeneous global industry using global distribution channels.

Businesses are capturing the ICT dividend; gaining efficiency and productivity but perhaps at the expense of basic security. Owners and operators of these infrastructures (e.g., water, finance, communications, transportation and energy installations and networks) are first and foremost worried about providing returns for shareholders, whereas a government's concern is with overall public security and safety.[135] Governments recognise that a disruption in one infrastructure can easily propagate into other infrastructures and that they are responsible for protecting the nation from catastrophic damage. Perhaps this is why, 'critical infrastructure services are regarded by some governments as national security related services.'[136]

The short-term economic gains of adopting new technologies and transforming the cyber infrastructure must be balanced against the medium and longer-term losses stemming from failing to adequately secure these systems and infrastructures.[137] While there a number of examples of this, the current discussions around modernising the electric power sector to internet-facing 'smart grids' is emblematic:

---

134 'Critical infrastructures are those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments' (See European Union, 'Critical infrastructure protection,' http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm.).

135 Peter Sommer and Ian Brown, Reducing Systemic Cybersecurity Risk, (Paris: OECD, 2011), http://www.oecd.org/sti/futures/globalprospects/46889922.pdf.

136 ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity,' 11.

137 Jack Goldsmith and Melissa Hathaway, 'The cybersecurity changes we need,' *The Washington Post*, 29 May 2010.

while the industry would reap great productivity gains, there are a number of serious unsolved security concerns. For example, 'smart meters with designated public IP addresses may be susceptible to denial of service attacks which could result in loss of communication between the utility and the meters and therefore deny power to homes and businesses.'[138] Thus, a potential 'modernisation' agenda is brought into direct conflict with a security agenda.

Deploying appropriate security measures to manage risk to critical systems and assets is costly. The question is: what are the most appropriate and effective security measures to manage risk to critical systems and assets and who pays for it? Owners and operators of these infrastructures have to play an active role in defining the standards that must be implemented to meet the government's mandate in assuring essential services. Industry also may be asked to make security investments that go beyond what is required to meet compliance and regulatory regimes. The policy intervention that a government uses to meet the needs of the nation must be carefully balanced to heighten cyber security without creating barriers to innovation, economic growth, and the free flow of information.

### 1.5.3. Private Sector vs. Public Sector

A critical feature of modern NCS is the role of the private sector. It is responsible for the research, design, development and manufacturing of the vast majority of software and hardware used in ICT. It has, in effect, become 'the' service provider; the steward of the internet that plans and manages resources, provides reliable connectivity, and ensures delivery for traffic and services.

Critical infrastructures and industries are increasingly the primary target of cyber crime, cyber espionage, and, most recently, serious cyber attack. Their electronic defences have been punctured and the potential costs of these activities are considerable. For example, the theft of intellectual property (which includes cyber espionage activity) is said to have cost the UK economy up to £9.2 billion in 2010.[139] Some adversaries have ambition to destroy or, perhaps worse, deliberately insert erroneous data to render systems inoperable and information unusable. The costs of these activities against the critical infrastructure are difficult to estimate, however, one industry report claimed that in the US 'the reported costs of downtime due

---

[138] Melissa Hathaway, 'Power Hackers: The U.S. Smart Grid Is Shaping Up to Be Dangerously Insecure,' *Scientific American*, 5 October 2010, 16.

[139] Detica, The Cost of Cyber Crime. A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, (London: UK Cabinet Office, 2011), http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf.

to cyber attacks exceed $6 million a day'.[140] In April 2009, the North American Electric Reliability Corporation (NERC) issued a public notice that warned that the electrical grid is not adequately protected from cyber attack: 'facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.'[141] Some observers have warned that a serious cyber attack on the US electrical grid could cause 'over $6 billion in damages,'[142] and the Commander of US Cyber Command said that, between 2009 and 2011, attacks on US critical infrastructures had 'risen 20-fold.'[143]

Governments have a clear interest in assisting the private sector in protecting the nation's essential services, wealth and growth potential (e.g., intellectual property protection) from these activities, but the ways and means of this assistance is fiercely debated. For example, some governments are choosing to regulate critical infrastructure providers by imposing minimum standards for technology deployment, internal security controls, and disaster recovery and business continuity plans. Whereas other government intervention options may include the provision of tax incentives, stimulus grants, low-cost or no-cost loans, government subsidies, insurance, and even liability protection. These incentives are meant to encourage industry participation in meeting the desired infrastructure objectives – to be both secure and resilient.

Either one of these options usually is supported by information exchanges, sometimes also referred to as the private-public partnership, that draw on combining the best of both party's understanding of the environment to support operational cyber security. For example, in some cases this includes pooling knowledge of tactics, techniques and procedures used to probe and successfully breach corporate and government networks.[144] Other information exchanges share counter-measure technologies and solutions to deny or investigate the cyber perpetrator.[145] Some governments even offer to help protect their critical infrastructure directly, by deploying sensors in the networks to (supposedly) detect the most advanced

---

140 Stewart Baker, Shaun Waterman, and George Ivanov, In the Crossfire. Critical Infrastructure in the Age of Cyber War, (Santa Clara, CA: McAfee, 2010), http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf.

141 Michael Assante, Critical Cyber Asset Identification [Letter to Industry Stakeholders], (Princeton, NJ: NERC, 2009), http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf.

142 John O. Brennan, 'Time to protect against dangers of cyberattack,' *The Washington Post*, 16 April 2012.

143 Jasmin Melvin, 'White House lobbies for cybersecurity bill amid worries it may stall,' *Reuters*, 1 August 2012.

144 See Critical Infrastructure Protection Initiative (CPNI): http://www.cpni.gov.uk/about.

145 INTERPOL, 'INTERPOL and ICANN advance cooperation on Internet security after historic first meeting,' *Media Release*, 23 May 2011.

threats.[146] These can be accompanied by encouraging the developments of voluntary codes of conduct, creating repositories of best practices, and encouraging private-sector initiatives to regularly test their systems' security posture and practice their recovery processes and procedures. Each of these initiatives helps build trust and understanding among and within the partnership and, perhaps more importantly, begins to promote education and awareness-raising across the nation.

While it remains unclear to what extent these measures actually help protect private business and the nation's networks, an equally contentious debate is being waged around the governmental approach to intervention in the private sector: either seeking voluntary cooperation or 'mandated' (i.e., prescribed by law or regulation). Understandably this involvement of the state in private affairs is a deeply ideological question in many nations. According to one 2009 study on European CIIP programmes,[147] of 16 EU Member States examined, around half favoured more voluntary than mandatory principles in their programmes, approximately six balanced voluntary and legal measures, and only two Member States seemed to largely or completely dependent on regulation. It is however very likely that this number has changed, given the recent European trend for applying legislation to the issue.

Most nations, however, agree that cyber security is a shared responsibility. The Director of the UK Government Communications Headquarters (GCHQ) recently argued that it is this 'holistic approach to cyber security that makes UK networks intrinsically resilient in the face of cyber threats.'[148] He went on to explain that this enhanced security posture would lead to a more competitive, economic posture for the nation.

### 1.5.4. Data Protection vs. Information Sharing

Another barrier to realising the full economic benefits of the internet economy involves the natural conflict between citizens' expectations and government policy for data protection and preserving privacy *vis-à-vis* the need to share information across boundaries and borders (e.g., government to industry, government to government, industry to industry) with the intent to enhance security. Enterprises of all kinds rely on the willingness of consumers and business partners to entrust them with private information. These constituents, in turn, expect that this information will stay both private and secure. Citizens expect protection from

---

146 Warwick Ashford, 'BT extends cyber security agreement with MoD,' *ComputerWeekly.com*, 4 July 2012.

147 Booz & Company, *Comparison and Aggregation of National Approaches (JLS/2008/D1/019 – WP 4)* (2009). 28.

148 BBC, 'UK infrastructure faces cyber threat, says GCHQ chief,' *BBC News*, 12 October 2010.

intrusions by both private and governmental actors. In 1980, the OECD issued a 'Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.'[149] The OECD guidelines influenced international agreements, national laws and self-regulatory policies.

This document sparked discussion around the world and, over the next three decades, different approaches to privacy policy and regulation emerged for reasons ranging from enhancing national security to negatively impacting economic growth. As one industry expert noted, 'providing seamless privacy protection for data as it flows through the global internet requires a careful reconsideration of the business community's interest in promoting commerce, the government's interests in fostering economic growth and protecting its citizens, and the interest of individuals in protecting themselves from intrusive overreach by government and the private sector.'[150] Today, many governments have established privacy rights for individuals, developed data protection frameworks and mandated privacy policies to preserve this notion of confidentiality.

Yet, countering crime, espionage, and other illicit activities in cyberspace demands timely exchange of warnings and follow up information among and between private and public entities, often exchanging sensitive data that may fall within the remit of these privacy and data protection laws. A major example of this dichotomy could be seen in Europe, where the 'European Data Retention Directive' (EDRD)[151] was in some ways the one of the most controversial pieces of EU legislation ever passed, and indeed is still being resisted by some EU Member States. Computer incident response centres and industry information security specialists argue that they need an information sharing mechanism that swiftly delivers alerts regarding tactics, techniques, and procedures used to probe and successfully breach victim networks. For some countries, this falls within the private-public partnership cooperation models where industry and government share the responsibility for security and resilience objectives. For example, the United States, the United Kingdom and other governments are providing actionable information and analysis regarding current threats to their industry. While not robust, these initiatives are trying to establish bi-directional information sharing architectures to accelerate better understanding or situation awareness about how industry or the nation overall is being targeted, what information is being lost, and the methods they

149 OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD, 1980).

150 CDT, 'Chapter Three: Existing Privacy Protections,' ed. CDT, *CDT's Guide to Online Privacy* (Washington, DC: CDT, 2009), https://www.cdt.org/privacy/guide.

151 The EDRD was adopted in 2006 and requires, among other things, that all ISPs keep their customer logs six months to two years to support criminal prosecution.

(industry and government) can use to defend their information assets, and respond to, and recover from significant incidents.

National laws may be insufficient, on their own, to provide citizens with privacy protections across borders while at the same time allowing for the timely exchange of threat information. This inherent tension lies at the heart of the cyber security debate.

### 1.5.5. Freedom of Expression vs. Political Stability

Recent news reports have illustrated how ICT and innovative use thereof can enhance or constrain the power of politicians and the general public. For some, ICT allows for widespread participation by citizens in day-to-day policy decisions. For example, in January 2012, US politicians faced widespread outrage regarding the Stop Online Piracy Act (SOPA), a bill that was introduced and debated before Congress.[152] Opponents to the bill stated that the proposed legislation threatened free speech and enabled law enforcement to block access to the internet due to copyright infringing (anti-piracy) content posted on web pages or blogs. On January 18, 2012, Wikipedia, Reddit, TwitPic and an estimated 7,000 other smaller websites coordinated a service blackout to raise awareness. The bill was quickly postponed for consideration due to this public pressure. In August 2011, during the England riots, some rioters used Blackberry Messenger to organise their activities and others utilised Twitter and Facebook to coordinate clean-up operations.[153] British officials used facial recognition software with social networks like Facebook to allow citizens to report rioters to authorities. In addition, social networking helped identify suspects and apprehend them for criminal damage, burglary, and violent disorder. A wider 'crackdown' on social media was narrowly avoided.[154]

ICT innovations also raise privacy concerns because governments and corporations can use 'digital surveillance technologies, such as networked webcams, location tracking, digital identification (ID) devices, data mining and analyses of communication traffic and search engine queries' to create digital dossiers of our citizens.[155] Activist groups such as Anonymous, LulzSec and WikiLeaks, expose victim's data to embarrass or achieve other objectives. However, the United States continues to push for equal access to knowledge and ideas across the digital

---

152 Ned Potter, 'Wikipedia Blackout,' SOPA and PIPA Explained,' *ABC News*, 17 January 2012.

153 BBC, 'England riots: Twitter and Facebook users plan clean-up,' *BBC News*, 9 August 2011.

154 See, for instance, Peter Apps, 'Analysis: UK social media controls point to wider 'info war',' *Reuters*, 18 August 2011.

155 Walter S. Baer et al., Machiavelli Confronts 21st Century Digital Technology: Democracy in a Network Society (Working Paper), (Oxford: Oxford Internet Institute, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1521222. 5.

frontiers of the 21st century: 'This freedom is no longer defined solely by whether citizens can go into the town square and criticise their government without fear of retribution. Blogs, e-mail, social networks and text messages have opened up new forums for exchanging ideas – and created new targets for censorship.'[156]

New technologies are being used to change the outcomes in the struggle for freedom and progress. The internet can be co-opted as a tool to target and silence citizens and it can be used to deny access to and use of key applications. For example, in early April 2012, the Iranian minister for Information and Communications Technology announced that Iran will field a national Intranet and begin blocking services like Google, Gmail, Google Plus, Yahoo and Hotmail, in line with Iran's plan for a 'clean internet.' These 'Western' services will be replaced with government internet services like Iran Mail and Iran Search Engine.[157]

In addition, during the early days of the social uprising that ultimately lead to the ousting of President Hosni Mubarak, the Egyptian telecommunications authority received an order from the security services to shutdown internet access. 88% of Egyptians lost access to the internet during this episode.[158] Other states in the region (e.g., Libya and Syria) implemented similar measures to try to maintain social stability as the 'Arab Spring' continued. While the acts of authoritarian regimes fighting for their political lives may seem extreme to many in the Western world, what these episodes demonstrate is that the very interconnectedness that people around the globe enjoy because of improvements in ICT can be swiftly denied, and that freedom of communication and political freedom are clearly linked.

## 1.6. CONCLUSION

Addressing a nation's cyber security needs is no easy task. Indeed, it is not even always apparent what those needs exactly are, or what protecting (or not protecting) a nation's cyber environment actually entails. Quite often there are different and competing considerations within each nation's approach. Yet each nation is faced with a steadily increasing level of cyber threat, and thus requires the nation's leadership to recognise the strategic problem and set forth goals and strategies to address it. In this section we have defined NCS as 'the focused application of specific governmental levers (which includes both incentives and regulation) and information assurance principles to public, private, and relevant international

156 Hillary R. Clinton, 'Internet Freedom [Speech at Newseum in Washington, DC],' *Foreign Policy*, 21 January 2010.

157 Amrutha Gayathri, 'Iran To Shut Down Internet Permanently; 'Clean' National Intranet In Pipeline,' *International Business Times*, 9 April 2012.

158 Christopher Williams, 'How Egypt shut down the internet,' *The Telegraph*, 28 January 2011.

ICT systems, and their associated content, where these systems directly pertain to national security.' As nations and intergovernmental organisations set about developing and implementing measures to establish NCS strategies, they must balance the economic and social importance of free flow of information to the security needs of government, industry, and citizens. The conceptual prism set forth in this section is designed to assist in this development and debate.

# 2. POLITICAL AIMS & POLICY METHODS

*Gustav Lindstrom, Eric Luiijf*

**Section 2: Principal Findings**

- There is growing convergence across national security strategies (NSS) with respect to identified threats and challenges (e.g., proliferation of weapons of mass destruction, terrorism, state failure, etc.).
- Most NSS include non-traditional threats, including a cyber security dimension. The cyber dimension is frequently recognised as cross-cutting a variety of critical infrastructure sectors and other sectors important to society (e.g., energy security).
- There are suggestions that political will (and understanding) is still limited when it comes to tackling cyber security risk factors.
- National cyber security strategies (NCSS) are used to provide guidance to policy-makers and other stakeholders regarding cyber security policy priorities and potential resource allocations. They can also form an important part of a nation's declaratory policy.
- Among the principal categories subject to cyber threats as identified in existing NCSS are critical infrastructures, economic prosperity, national security, and societal well-being.
- An examination of 19 NCSS suggests there are diverging understandings of cyberspace. Some equate it closely to the internet while others embrace a broader definition.
- Less than half of the NCSS examined define terms like 'cyber security'.

## 2.1. INTRODUCTION

Concepts of national and international security have changed considerably since the end of the Cold War. In particular, there has been a noticeable shift from the concept of combating specific threats to reducing and mitigating risk factors to society as a whole. As noted by NATO in its 1991 Strategic Concept:

> 'The primary role of Alliance military forces, to guarantee the security and territorial integrity of member states, remains unchanged. But this role must take account of the new strategic environment, in which a single massive and global threat has given way to diverse and multi-directional risks.'[159]

Starting in the mid-1990s, the notion of 'Comprehensive Security' (originally put forward by the OSCE[160] in 1990) became more prominent. This concept facilitated a broader and deeper interpretation of security needs and requirements, and helped inform the idea of 'enhanced' or 'expanded security' that identified security policy dimensions in other domains such as food, health and the environment.[161] The recognition that security was fundamentally more than the territorial integrity of the state led to an even more radical shift. The Human Security concept (developed mostly under the aegis of the UN)[162] directly questioned the 'state-centric' approach to security, and put the needs of the individual first. The rise of Human Security as a concept had a direct influence on the more 'state-centric' approaches of Comprehensive or Expanded Security as well.[163] On the one hand it helped launch the notion of 'individual' or 'societal' needs, and how national security could be re-conceptualised as being primarily orientated to help meet the satisfaction of these needs through variously defined 'services'. On the other hand, it was increasingly recognised that threats and risks to these societal needs were not easily categorised as being primarily an 'internal' or 'external' security issue.

The need to create a more unified approach to meet a variety of security challenges, coupled with the need to do so with limited resources, was a principal driver for the introduction of national security strategies in the late 1990s and the early 2000s.

### 2.1.1. Aims of National Security Strategies

The formulation of national security strategies (NSS) is a relatively recent phenomenon. Presently, a majority of countries possessing a national security strategy can trace their initial security strategy to the late 1990s or early 2000s. In the United States, one of the earliest developers of a NSS, initial concepts and

---

159 NATO, *The Alliance's New Strategic Concept* (London: NATO, 1991).

160 OSCE, *The OSCE Concept of Comprehensive and Co-operative Security. An Overview of Major Milestones (SEC/CPC/OS/167/09)* (Vienna: OSCE, 2009).

161 For a discussion on the development of various security concepts in Europe and the Mediterranean Area, as well as the role of NATO, see: Hans G. Brauch et al., *Security and Environment in the Mediterranean: Conceptualising Security and Environmental Conflicts*(Berlin et al.: Springer Verlag, 2003).

162 UNDP, Human Development Report 1994. New Dimensions of Human Security, (Oxford and New York: Oxford University Press, 1994), http://hdr.undp.org/en/reports/global/hdr1994.

163 For a discussion on the development of expanded security and Comprehensive Security concepts during the early 1990s, see Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009). 136-37.

policy statements were already formulated in the late 1940s.[164] A facilitating factor was the signing of the 1947 National Security Act which, among others, set up the National Security Council. In 1986, through the Goldwater-Nichols Department of Defense Reorganization Act, the US made the formulation of a NSS a requirement.

Outside of the United States, the introduction of NSS has been a fairly recent development. Establishing a NSS has substantial appeal because it encourages policy-makers to identify strategic objectives ('ends'), to pinpoint the resources available to reach those objectives ('means'), and to provide a guide on how such resources are to be applied to reach stated objectives ('ways'). Ideally, a NSS contains strategic objectives that are consistent with national values and interests. As an overarching strategic document, a NSS often includes political, internal security, foreign policy, defence structures and economic dimensions.

A well-formulated NSS should do at least three things. Firstly, it should enable government departments and ministries to translate a government's national security vision into coherent and implementable policies. It should also facilitate the production of 'sub-strategies' across different domain areas that are consistent with the overarching NSS (e.g., a strategy for combating terrorism). Since most NSS highlight resources needed to achieve national security objectives, they should likewise provide guidance on R&D in new security capabilities, future procurements, investments, and budget decisions. Ultimately, a NSS is the 'peak' national security document for a government, sited at the apex of a whole set of different policy documents that – ultimately – should refer back and get their guidance from the NSS.[165]

Secondly, a NSS should clarify how the state might act in international affairs – enabling a more proactive rather than reactive foreign policy. To illustrate, a NSS could be helpful in determining what elements of national power (e.g., diplomatic, information, military, economic) are most likely to be employed to reach specific international objectives. Besides informing international policy making, a NSS should serve to communicate strategic thinking to other states and the international community at large.

---

164 See, for instance, US National Security Council, *NSC 68: United States Objectives and Programs for National Security* (Washington, DC: FAS, 1950). This document was declassified in 1975. As a *de facto* NSS, NSC 68 shaped US foreign policy substantially during the Cold War era.

165 Although the hierarchies can be relatively difficult to establish, one example of such a document progression would be from the UK: The UK Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world.* informed the UK Cabinet Office, *Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space.*, which, in turn, provided the frame for the UK Home Office, *Cyber Crime Strategy* (Norwich: The Stationery Office, 2010).

Thirdly, a NSS should not exist in a strategic vacuum. On the contrary, it should be linked to existing national and international strategies to the extent that it is feasible to encourage a harmonised set of policies that are shared with likeminded partners. The linking of a NSS with other strategies may also be helpful to promote coordination, cooperation and collaboration. At the international level, it may also serve to facilitate a Whole of System approach (examined in greater detail in Section 3).

A NSS usually contains both explicit and implicit elements. Most current documents tend to be fairly explicit with respect to perceived threats and challenges, even if the understanding of the term 'national security' may differ from country to country or evolve over time. While strategies typically outline threats and challenges, they may be less forthcoming on which threats are of greatest concern. Likewise, strategies are usually less explicit when it comes to how the government may address identified threats and challenges, including resources that may be necessary or questions about which departments should take the lead in response.[166] This is not altogether surprising since a NSS usually serves to provide strategic guidance to government ministries and agencies. Ambiguity concerning policy responses may also be useful to discourage potential adversaries from engaging in certain behaviours or actions.

### 2.1.2. Trends in National Security Strategy Formulation

An examination of current national security strategies suggests four trends. First, there seems to be a growing convergence among policy-makers with respect to the key threats and challenges facing states. As shown in Table 4, examples of oft-cited threats and challenges include the proliferation of weapons of mass destruction, terrorism, state failure, and organised crime, besides, of course, cyber security threats.

There may be several explanations for this trend. For example, convergence with respect to threats and challenges across countries' NSS may arise when policy-makers are formulating a NSS to analyse existing strategies and use elements of those strategies as a basis for their own strategic reflection. Another factor may be the global impact of events such as terrorist attacks (the 9/11 attacks in New York and Washington D.C., the Madrid train bombings in March 2004, and the London transport attacks in July 2007, etc.) that have led policy-makers to converge on a shared set of security threats and challenges.

---

166 Catherine Dale, National Security Strategy: Legislative Mandates, Execution to Date, and Considerations for Congress, (Washington, DC: Congressional Research Service, 2008), http://fpc.state.gov/documents/organization/106170.pdf.

**Table 4:** Comparison of Threats and Vulnerabilities: Select NATO Member States Security Strategies/White Books

| Country | Document type | Year | Examples of Threats / Vulnerabilities |
|---|---|---|---|
| **France** | White Book | 2008 | 'Weapons of Mass Destruction' (WMD); terrorism; ballistic missile proliferation; cyber attacks; espionage; criminal networks; health risks; citizens abroad in vulnerable areas |
| **Germany** | White Book | 2006 | International terrorism; proliferation and military build-up; regional conflicts; illegal arms trade; fragile statehood; transportation routes; energy security; uncontrolled migration; epidemics and pandemics |
| **Hungary** | Security Strategy | 2012 | Terrorism; proliferation of WMD; unstable regions/failed states; illegal migration; economic instability; challenges to information society; global natural, man-made and medical sources of danger; regional challenges; internal challenges |
| **Netherland** | Security Strategy | 2007 | Breaches of international peace and security; 'chemical, biological, radiological, and nuclear' (CBRN); terrorism; international organised crime; social vulnerability; digital lack of security; economic lack of security; climate change and natural disasters; infectious diseases and animal diseases |
| **Poland** | Security Strategy | 2007 | Organised international terrorism; organised international crime; energy security; illegal migration; weakened transatlantic links; frozen and regional conflicts; weak levels of integration of economic life and financial markets; environmental threats; internal challenges (e.g., population changes, infrastructure, energy storage) |
| **Spain** | Security Strategy | 2011 | Armed conflicts; terrorism; organised crime; financial and economic insecurity; energy vulnerability; proliferation of weapons of mass destruction; cyber threats; uncontrolled migratory flows; emergencies and disasters; critical infrastructures; supplies and services |
| **United Kingdom** | Security Strategy | 2010 | International terrorism; hostile attacks upon UK cyberspace; major accident or natural hazards; an attack on the UK or its overseas territories; risk of major instability; organised crime; severe disruption to satellite communications; disruption to oil or gas supplies; short to medium term disruption to international supplies of essential resources |
| **United States** | Security Strategy | 2010 | WMD; space and cyberspace vulnerabilities; energy dependence; climate change; pandemic disease; failing states; global criminal networks |

A related development explicit in some NSS (e.g., the United States and the United Kingdom) is the recognition that a diverse set of threats and challenges requires an integrated all-hazards risk management approach.[167] Taking a broader perspective, policy-makers and analysts embracing this concept are more inclined to examine national vulnerabilities, gauge the possible consequences of a threat, and seek innovative ways to protect society as a whole. Reinforcing the trend towards risk management is the realisation that national means are not unlimited, requiring a more careful analysis of where and how finite means should be employed.

The shift to a national risk management paradigm is visible in those NSS that highlight the need to enhance national resilience or underscore the importance of incorporating an 'all-hazards' approach. While the overarching goal of achieving comprehensive security remains (and some might argue is promoted), this development acknowledges that achieving a 100% protection level is neither feasible not realistic. Thus the need to identify new defensive and mitigating measures to provide security.

A second trend, related to the first point, is that national security strategies are identifying 'new' threats and challenges. As noted earlier, a broader understanding of the term 'security' is likely contributing to this trend.[168] Table 4 provides some illustrations such as climate change, energy supply, health risk, and cyber security. The inclusion of these challenges is often accompanied by the recognition of their complexity and far-reaching implications. The case of climate change, for instance, is considered a long-term challenge whose impact may not be felt for several decades. However, addressing it requires action today, preferably in a collective manner at the international level. Complicating these efforts is the perception that the effects of climate change may be more severe on some parts of the world than in others, leading to more disparate cooperation. With respect to cyber security, it is frequently included in new NSS as a 'new' threat. Its inclusion or perceived importance, however, does not necessarily translate to increased awareness at the senior policy level of the scope of the challenge. While there is no authoritative international survey of government decision-makers and senior policy-makers with respect to their perception of the cyber security challenge, there are suggestions that political will is still limited when it comes to tackling cyber security risk factors. For example, while policy-makers agree that international cooperation is necessary

---

167 According to the Department of Homeland Security Risk Lexicon, defined as the 'incorporation and coordination of strategy, capability, and governance to enable risk-informed decision making (see US Department of Homeland Security, DHS Risk Lexicon, (Washington, DC: Risk Steering Committee, 2008), http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf. 19.).

168 A school of academic thought (the Copenhagen School) has forwarded the concept of 'securitisation' to reflect the tendency of a broader understanding of the concept of security. For more, see Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security. A New Framework For Analysis* (London: Lynne Rienner Publishers, Inc., 1998).

to mitigate cyber challenges, a 2010 survey of policy-makers, specialists, business executives, community leaders and journalists carried out by the EastWest Institute indicates that little is being done: 'Track 1 diplomacy on worldwide cybersecurity cooperation is not working well on the tactical level and practically non-existent on the strategic level.'[169] Underscoring the importance of political will, 36% of those surveyed saw political/policy as the key ingredient to address principal cyber challenges, followed by 27% identifying technical solutions, 16% listing business and legal measures (for each), with the remaining 5% singling out legal means.[170]

It is important to note that decision-makers' and policy-makers' perceptions can change quickly. This was most visible in the aftermath of the distributed denial of service (DDoS) attacks on Estonia in April/May 2007, after which cyber security issues increasingly entered the political agenda. The release of national cyber security strategies (many of which came out in 2009-2011) also point in the direction of a greater acknowledgement of the relevance of cyber security. A 2012 report by McAfee and the Brussels based Security & Defence Agenda[171] that surveyed policy-makers in several countries found that 45% of respondents believe cyber security is as important as border security.[172]

A third trend with respect to the formulation of a NSS is a greater awareness of the link between internal and external security. In the aftermath of 9/11 and coupled with the identification of new threats such as pandemics, it became increasingly evident that internal and external security should be considered more in tandem, especially as risk factors and challenges from the outside do not necessarily stop at external borders. The reverse may be true as well. For example, a set of cartoons in a local newspaper in Denmark led, over time, to major internal security events in several other nations external to Denmark. It included, for instance, arson attacks on a Danish embassy and people rioting in other nations.

A stronger, more dynamic link between internal and external security in existing NSS has wide-ranging implications for policy-makers. Among others, it highlights the need for greater cooperation across government departments, especially those that deal with internal security (interior and justice) and those that handle external security (foreign affairs and defence). It also requires policy-makers to

---

169 EastWest Institute, International Pathways to Cybersecurity. Report of Consultation, (Brussels: EastWest Institute, 2010), http://www.ewi.info/system/files/CyberSummaryReport.pdf. 1.

170 Ibid., 3.

171 Brigid Grauman, Cyber-security: The vexed question of global rules. An independent report on cyber-preparedness around the world, (Brussels: Geert Cami, 2012), http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf.

172 Specifically, the survey included in-depth interviews with 80 policy-makers, cyber security experts in government, business and academia in 27 countries. Also surveyed were 250 'world leaders' in 35 countries. For more information, see ibid.

think carefully about how resources might be allocated to satisfy internal and external security objectives. For some, a stronger connection between internal and external security may translate into a more active foreign policy ('best defence is a good offence'). Others may perceive the need to strengthen internal security and resilience to better withstand external security challenges. For all these reasons, the establishment of a NSS is increasingly becoming an interagency project that can provide a holistic vision for national security.

A fourth point is that, while most NSS traditionally include a security, political and economic dimension, present-day NSS go a step further by clearly recognising the need to combine traditional security policies, development cooperation policies, and economic tools at large to promote security and development. The combination of civilian and military assets is also encompassed in new concepts such as civil-military coordination (CMCO) and the 'Comprehensive Approach'.[173]

This trend underscores the dynamic and changing nature of NSS. It also points to a greater recognition that a combination of different tools is required to address 21st century threats and challenges. To a certain degree, this development is not surprising given the inclusion of both traditional and non-traditional security threats in NSS. Over time, capturing the complexity of the international security landscape is likely to strengthen the role of having a NSS as a strategic platform to derive follow on strategies and policies.

### 2.1.3. Integrating Cyber Security in National Security Strategies

As noted in Section 1, several NSS include a cyber security dimension. The references made to the cyber domain can take several forms. A majority of the NSS identify cyber threats as a new security challenge that policy-makers should be aware of. Many also highlight that the cyber domain can impact other sectors or domains, e.g., energy, health and environment. As a cross-sector issue, it is important to discern both the enabling characteristics of cyber across different domains as well as potential risk factors.

Some strategies go a step further by identifying a particular cyber security dimension that is of concern. An example that is visible in some strategies is the need to protect 'critical infrastructures' (CI) – i.e., those utilities and services that are necessary to maintain societal needs, such as electric power, communications, but also banking. Countries such as France and the UK integrate a cyber dimension

[173] Some analysts also like to include concepts such as 'Civil-Military Cooperation' (CIMIC) which focuses on how deployed military elements best interact with civilian counterparts to achieve desired effects.

more extensively into their overall security planning, for example by providing details on major cyber attacks and their application for espionage (France)[174] as well as the benefits cyberspace offers to industry, government and the general population (UK).[175] The UK NSS also notes that cyber attacks are considered among the four high priority risk factors over the next five years. In the case of the Spanish NSS, an entire section is dedicated to cyber threats which also describe specific lines of action that can be considered in response to a cyber threat.[176]

As noted earlier, in the aftermath of the distributed denial of service attack on Estonia in April 2007, the cyber dimension took on a more prominent role. The media coverage of specific supposed state-sponsored malicious software (such as Stuxnet, Duqu and Flame) and cyber espionage attacks on various nations and international organisations is likely to further attune countries to the importance of cyber security, especially with respect to critical information infrastructure protection (CIIP).[177] Looking ahead, the cyber security dimension will increasingly be covered in stand-alone NCS strategies.

The overall trend can be summarised as follows: most recent NSS documents acknowledge the need to address cyber security, and give this issue the highest priority compared with other risks. Sometimes, as in the United States NSS of 2010, they will deal with cyber security both as its own discrete element, but also as a horizontal issue that crosses a number of other NSS goals.[178] In nearly all cases there will be subsequent and subordinate documents that deal specifically with the threat to national cyber security and, subordinate to that, specific documents addressing specific cyber threats, such as within a military or law enforcement environment.

---

174 French Secretariat-General for National Defence and Security, *Information systems defence and security. France's strategy.*

175 UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.*

176 Spanish Government, *Spanish Security Strategy. Everyone's responsibility* (Madrid Spanish Government, 2011). 60-4.

177 Sometimes abbreviated as CI(I)P. Some countries use CIIP as a clear sub-category to overall CIP; while other countries equate CIIP to NCS.

178 Within the US NSS 2010, one specific goal is mentioned: 'Secure Cyberspace'. However, 'cyber' is mentioned at least as often among other NSS goals as within the specific 'Secure Cyberspace' goal (see White House, *National Security Strategy.*).

## 2.2. THE NATIONAL CYBER SECURITY DIMENSION

### 2.2.1. Themes in National Cyber Security Strategies

To date, over 20 states have released a national cyber security strategy (NCSS) or national information security strategy, many of them unveiling one in 2011.[179] With respect to NATO members, nearly half have produced a NCSS that details national visions, guiding principles, perceptions of the threat, and strategic objectives.[180]

**Table 5:** Examples of National Cyber Security Strategies

| Nation | Issued | Lead Agency | English version | Other languages |
|---|---|---|---|---|
| **Australia** | Nov 2009 | Attorney-General | Cyber Security Strategy[181] | - |
| **Canada** | Oct 2009 | Public Safety Canada | Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada[182] | French |
| **Czech Republic** | Jul 2011 | Ministry of Interior | Cyber Security Strategy of the Czech Republic for the Period 2011-2015[183] | Czech |
| **Estonia** | Sep 2008 | Ministry of Defence | Cyber Security Strategy[184] | Estonian |
| **France** | Feb 2011 | General Secretariat for Defence and National Security | Information systems defence and security. France's Strategy[185] | French |

[179] Among these are Australia, Canada, the Czech Republic, Estonia, France, Germany, India, Japan, Lithuania, Luxembourg, the Netherlands, New Zealand, Romania, Slovakia, South Africa, South Korea, Spain, Switzerland, Uganda, the United Kingdom and the United States. Countries in the process of finalising their NCSS include Austria, Finland and Turkey.

[180] For an overview of these see Eric Luiijf, Kim Besseling, and Patrick De Graaf, 'Nineteen National Cyber Security Strategies,' *International Journal of Critical Infrastructures* (forthcoming).

[181] Australian Attorney-General's Department, *Cyber Security Strategy.*

[182] Canadian Department for Public Safety, *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada.*

[183] Czech Ministry of Interior, *Czech Cyber Security Strategy for the Period 2011–2015 (Prague: ENISA, 2011).*

[184] Estonian Ministry of Defence, *Cyber Security Strategy* (Tallinn: Estonian Ministry of Defence, 2008).

[185] French Secretariat-General for National Defence and Security, *Information systems defence and security. France's strategy.*

| Nation | Issued | Lead Agency | English version | Other languages |
|---|---|---|---|---|
| **Germany** | Feb 2011 | Federal Ministry of the Interior | Cyber Security Strategy for Germany[186] | German |
| **India** | Apr 2011 | Ministry of Communications and Information Technology | Discussion Draft on National Cyber Security Policy[187] | - |
| **Japan** | May 2010 | Information Security Policy Council | Information Security Strategy for Protecting the Nation[188] | Japanese |
| **Lithuania** | Jun 2011 | Government of the Republic of Lithuania | Programme for the Development of Electronic Information Society (Cyber-Security) for 2011-2019[189] | Lithuanian |
| **Luxembourg** | Nov 2011 | Government of the Grand Duchy of Luxembourg | Not available online | French[190] |
| **Netherlands** | Feb 2011 | Ministry of Security and Justice | The National Cyber Security Strategy (NCSS). Strength through Cooperation[191] | Dutch |
| **New Zealand** | Jun 2011 | Ministry of Economic Development | New Zealand's Cyber Security Strategy[192] | - |
| **Romania** | May 2011 | Ministry of Communications and Information Society | Not available online | Romanian[193] |

186 German Federal Ministry of the Interior, *Cyber Security Strategy for Germany.*

187 Indian Ministry of Communications and Information Technology, *Discussion Draft on National Cyber Security Policy (New Delhi: Government of India, 2011).*

188 Japanese Information Security Policy Council, *Information Security Strategy for Protecting the Nation (Tokyo: National Information Security Center, 2010).*

189 Lithuanian Government, R*esolution NO 796 on the Approval of the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019* (Vilnius: Information Technology and Communications Department, 2011).

190 Luxembourg Government, *Stratégie nationale en matière de cyber sécurité (*Luxembourg: Government of the Grand Duchy of Luxembourg, 2011).

191 Dutch Ministry of Security and Justice, 'The National Cyber Security Strategy (NCSS). Strength through Cooperation.'

192 New Zealand Ministry of Economic Development, *New Zealand's Cyber Security Strategy* (Wellington: New Zealand Ministry of Economic Development, 2011).

193 Ministry of Communications and Information Society, *Strategia de securitate cibernetica a României* (Bucharest: Ministry of Communications and Information Society, 2011).

| Nation | Issued | Lead Agency | English version | Other languages |
|---|---|---|---|---|
| **Slovakia** | 2008 | Ministry of Finance | Slovak National Strategy for Information Security[194] | Slovakian |
| **South Africa** | Feb 2010 approved Mar 2012 | Department of State Security | Notice of Intention to Make South African National Cybersecurity Policy[195] | - |
| **South Korea** | Aug 2011 | Korea Communications Commission | - | Korean[196] |
| **Spain** | May 2011 | Spanish Government | Part of Spanish Security Strategy: Everyone's responsibility[197] | Spanish |
| **Switzerland** | Jun 2012 | Federal Department of Defence, Civil Protection and Sport | National Strategy for Protection of Switzerland against Cyber Risks[198] | German;[199] French |
| **Uganda** | Nov 2011 | Ministry of Information and Communication Technology | National Information Security Strategy[200] | - |
| **United Kingdom** | Nov 2011 | Cabinet Office | The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world[201] | - |
| **United States** | Feb 2003 | White House | The National Strategy to Secure Cyberspace[202] (also CNCI, HSPD-7, 60 day Review) | - |

194 Referenced by: http://www.webcastlive.es/4enise/archivos/T14/T14_Daniel_Olejar_CominiusUniversity.pdf.

195 South Africa Department of Communications, *Notice of Intention to Make South African National Cybersecurity Policy (Draft approved 11 March 2012)* (Pretoria: South Africa Government, 2010).

196 Not available online.

197 Spanish Government, *Spanish Security Strategy. Everyone's responsibility.*

198 Publication expected second half of 2012.

199 Swiss Federal Department of Defence, Civil Protection, and Sports, *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken* (Bern: Swiss Confederation, 2012).

200 Uganda Ministry of Information and Communications Technology, N*ational Information Security Strategy (NISS Final Draft)* (Kampala: Uganda Ministry of Information and Communications Technology, 2011).

201 UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.*

202 White House, *The National Strategy to Secure Cyberspace.*

The analysis of 19 NCSS by Luiijf et al. shows that several key themes and visions are highlighted across those strategies. Among the most recurrent are:

- Maintaining a secure, resilient, and trusted electronic operating environment,
- Promoting economic and social prosperity/promoting trust and enable business and economic growth,
- Overcoming the risk of information and communications technologies, and
- Strengthening the resilience of infrastructures.

The visions are translated into strategic objectives which are broken down further into a wide variety of priorities. With respect to the vision of maintaining a secure cyberspace, some countries express the need to raise awareness of the cyber risk, secure government systems, adopt an appropriate regulatory framework, modernise the legal framework, tackle cyber crime, or reinforce critical infrastructures. These and related objectives are also thought to contribute to economic prosperity by promoting trust and resilience.

There are differences in how states translate their visions into strategic objectives. A principal explanatory factor behind this may be countries' diverging understanding of cyberspace. Some countries take a broad view of cyberspace that includes infrastructures (such as control systems in critical infrastructures) and others take a much narrower view of cyberspace, equating it more closely to the internet. To illustrate, the United States is at one end of the spectrum with a broad definition of cyberspace, even implicitly acknowledging the importance of social networks.[203] In the Dutch NCSS, cyberspace is likewise defined broadly, including chip cards and in-car systems.[204] On the other side of the spectrum, countries like Australia, Canada, Germany, New Zealand and Spain place an emphasis on the internet and internet connected information technologies (additional details are provided in Section 2.3.1).

Beyond diverging perceptions of key concepts such as cyberspace, existing NCSS tend to have varying views on cyber threats. Among the principal cyber threat categories identified in existing NCSS are threats to:

- Critical infrastructures,
- Economic prosperity,
- National security,

---

[203] See Section 1.

[204] Luiijf, Besseling, and Graaf, 'Nineteen National Cyber Security Strategies.'

- Societal well-being,
- Public confidence in information and communication technologies,
- Economic prosperity, and
- Globalisation.

While some of these categories are acknowledged in all or most NCSS (e.g., cyber threats to critical infrastructures) some categories – such as threats to globalisation or societal well-being – are described explicitly or implicitly in few strategies.[205]

Existing NCSS also identify the sources of cyber threats. Among the principal dimensions identified are cyber threats via large-scale attacks, terrorists, foreign nations, espionage, organised crime, or political activism against ICT-based services. Some threat categories – such as cyber threats from organised crime – are highlighted in most NCSS. Other dimensions, such as threats from activists or extremists, figure in a couple of NCSS. The four categories referenced most frequently across the examined NCSS were organised crime, cyber threats from foreign nations (cyber war), cyber threats associated with terrorists, and espionage.[206]

Overall, roughly half of the NCSS examined demonstrate a direct link with the states' NSS. Most often, this takes the form of a reference to the NSS' identification of cyber as a potential security challenge or an acknowledgement of security objectives outlined in the NSS. It is, however, more difficult to gauge the different NCSS' relationship with other strategies and policies of importance. It is expected that such linkages become more reinforced over time. Factors that might expedite such a process range from refining the definitions of key concepts used in NCSS to strengthening the potential for public-private cooperation in the cyber domain.

An issue for future consideration is how existing NCSS can cope with rapidly changing threat dynamics. In other words, with no formal review mechanism in place, many NCSS may become irrelevant or unable to provide guidance when facing a new type of cyber challenge. Only a few countries have released more than one NCSS.[207] For example in the United States, several NCSS-type documents have been released.[208] In light of this limitation, it is interesting to note that some

---

205 Ibid.

206 Ibid.

207 Japan, for instance, has released a second version of a NCSS, but it mainly represents a refinement of the initial strategy. The UK revised its 2009 NCSS after a political signature change.

208 For a complete overview, see Rita Tehan, Cybersecurity: Authoritative Reports and Resources, (Washington, DC: Congressional Research Service, 2012), http://www.fas.org/sgp/crs/misc/R42507.pdf.

countries such as Germany and Japan indicate in their NCSS that there is a risk of a mismatch between technology development and security policy.[209]

## 2.2.2. Aims and Addressees

Consistent with other sub-strategies developed in support of a NSS, a NCSS aims to provide guidance to policy-makers regarding cyber policy priorities and potential resource allocations. However, these NCSS can also have other roles as well: they can play an active role in shaping the international image of a nation, and indicate where it thinks future collaboration would be possible. Within this context, a NCSS is a vital document for international partners to discern what the actual administrative responsibilities and whom the likely interlocutors are. A NCSS – or, indeed, a subordinate document focusing on the international cyber issues[210] – is a prerequisite to be actively able to engage with a nation's friends and allies on the issue.

In addition, a NCSS can form an important part of a nation's declaratory policy – indicating to potential adversaries where red lines may be drawn before retaliation can be expected, and what capabilities exist, or are being developed, to execute this type of policy. For instance, the United States has repeatedly warned that it would consider a serious cyber attack an 'act of war'.[211] The Russian Information Security Doctrine of 2000 makes it clear that 'an information attack' is not confined to cyber attack, but indeed can mean any kind of severe criticism of the Russian government.[212]

There are also less obvious components of a NCSS that are often intended purely for specialist observers. While these often depend on interpretation, they can be among the most significant. For example, one recent NCSS implied that a particular state had achieved a breakthrough in signal intelligence decryption technology, which facilitated real time cyber attribution. Although this statement is open to interpretation, if accurate, it would have significant implications for the entire nature of inter-state cyber conflict. In a related vein, many NCSS and associated documents are used to specify declaratory policy on cyber retaliation.[213]

---

209 Ibid.

210 One such example is: White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World.*

211 Most recently in the US DoD Cyber Strategy, commented on in the Wall Street Journal (see Siobhan Gorman and Julian E. Barnes, 'Cyber Combat: Act of War,' *The Wall Street Journal*, 30 May 2011.).

212 See, for instance, Alexander Klimburg, 'Mobilising Cyber Power,' *Survival* 53, no. 1 (2011): 41-60.

213 For some further notes on this, see Jason Healey, 'Bringing a Gun to a Knife Fight: US Declaratory Policy and Striking Back in Cyber Conflict,' *Atlantic Council Issue Brief*, September 2011.

With respect to cyber threats, vulnerabilities and measures, existing NCSS target a number of stakeholders. Principal among them, in terms of explicit mention in different NCSS, are government/national security officials, critical infrastructure operators, and citizens. Given the important link between the public and private sectors *vis-à-vis* cyber security, other stakeholders addressed in NCSS tend to be large organisations and small- and medium-sized enterprises. Both are mentioned explicitly in the NCSS by 11 out of the 19 nations examined by Luiijf et al.[214] A final stakeholder category, the Internet Service Providers, is acknowledged in one third of existing NCSS, perhaps somewhat surprising given their potential role in addressing cyber threats and vulnerabilities.

## 2.3. IMPLEMENTING CYBER SECURITY STRATEGIES

### 2.3.1. The Use of Terms

One of the findings by Luiijf et al.,[215] in studying 19 NCSS is that less than half of the nations explicitly define terms such as 'cyber security' in their NCSS. Some of the other nations explain cyber security in a descriptive text. One third of the nations, however, discuss cyber security without defining the term at all. The European Network and Information Security Agency (ENISA) observed the same lack of definitions, and presents recommendations to remediate that in the Member States of the European Union.[216]

Early in 2011, the Russian-US bilateral working group of the East West Institute (EWI) and Moscow University drafted an international cyber terminology framework. They defined cyber security as 'a property of cyberspace that is an ability to resist intentional and unintentional threats and respond and recover'.[217] The term 'cyber crime' is defined by only three of 19 NCSS studied by Luiijf et al., neither does the Convention on Cybercrime, ratified by many nations, define it.[218] It would appear that only Romania defines all cyber-related terms in its NCSS.

---

214 Luiijf, Besseling and Graaf, 'Nineteen National Cyber Security Strategies.'

215 Ibid.

216 ENISA, National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace, (Heraklion: ENISA, 2012), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport. 12-3.

217 EastWest Institute and Moscow State University, Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations, (Brussels and Moscow: EastWest Institute and Moscow State University, 2011). 31.

218 Council of Europe, *Convention on Cybercrime (ETS No. 185).*

In general, a national strategy may have different objectives: (1) to align the Whole of Government, (2) to coherently focus and coordinate public and private planning, and to convey the envisioned roles, responsibilities and relationships between all stakeholders, and (3) to convey one's national intent to other nations and stakeholders.[219] Examples of (3) are power projection and posing the national strategy as intent to become the lead nation or global player in the specific domain, or in global cyber security in the case of a NCSS.

The lack of properly defined cyber-related terms can lead to a significant level of confusion within one's own country. Moreover, as the cyber threat is global, proper definitions assist in understanding the cyber security approach of other nations, alliances, and international organisations and vice versa. For that reason, a NCSS without a properly defined, and, if possible, internationally harmonised cyber terminology framework, fails to meet any of the three objectives. The best approach is, therefore, to align one's national definition to the harmonised understanding of other nations.

### 2.3.2. The Role of Transparency

Depending on the political objective behind the NCSS, the NCSS may be largely strategic, or may include a list of operational and even tactical objectives to be accomplished.[220] To date, many of the strategies that have included a specific task listing have assigned a classified status to most of the document – this, for instance, was originally the case in the UK and the US examples. As far as relatively detailed NCSS are concerned, only the Netherlands' NCSS provides a fairly detailed, unredacted view of the activities proposed. Sometimes specifics are released after a short period of time: the US Comprehensive National Cybersecurity Initiative (CNCI) featured a list of 18 initiatives initially and only 12 of those have been made public.[221]

Transparency within cyber security, however, means more than listing the goals of the strategy. In an optimal case it would disclose the process behind a strategy, allowing outside observers to take stock of the individual steps involved, and potentially remove any doubt about the specifically stated aims within the strategy.

Another form of transparency is to make the NCSS online and available to one's own population and globally by providing an English-language version. As Table 5

---

219 Luiijf, Besseling, and Graaf, 'Nineteen National Cyber Security Strategies,' 2.

220 Ibid., 15.

221 See White House, *The Comprehensive National Cybersecurity Initiative (as codified in NSPD-54/HSPD-23).*

shows, most nations except Slovakia and South Korea provide an online version of their NCSS. Luxembourg and Romania do not provide an English translation.

### 2.3.3. Addressing Stakeholders

Nations use different structuring, types of wording, and layouts in their NCSS depending on the intended audience. Accessibility, therefore, ranges from large blocks of text for the purpose of aligning the Whole of Government, to a layout with photos and explanatory call out boxes to make the NCSS accessible for the general public, SMEs (Small and Medium Size Enterprises) and other businesses. Also, the historical, cultural, legal, organisational and political structure of a nation can lend to significant differences in working with stakeholders, ranging from a cooperative approach, public-private partnership, to mandatory legislation and regulation. Therefore, it is not just a simple copy and paste of policies, organisational structures, procedures and processes. A transposition to one's own national frameworks is required.[222]

Internal stakeholders such as critical infrastructure operators are often addressed through specific (traditional stovepiped) legislation and regulation mechanisms of bodies like the European Union, and specific regulators/regulatory commissions in various countries. Most liberal-democratic nations depend upon varying degrees of a stick-and-carrot approach where, through public-private partnerships, the private sector is allowed to regulate its own security posture as long as the public sector perceives there to be a good overall cyber governance structure. If the private sector fails to accomplish this on its own, the government steps in and tightens its cyber security legislative and regulatory frameworks.

An important factor in encouraging the private sector is the overall level of cyber security literacy and awareness. The importance of this issue is explicitly recognised by most NCSS. However, NCSS often have difficulty addressing the amorphous groups concerned and mostly simply state that organisations and individual citizens are responsible for a proper level of cyber security without going into detail. More significantly, there is often no particular government stovepipe that is responsible for following-up with detailed sub-strategy on this issue. Either the issue is treated only within CIP programmes and therefore not communicated to the public at large, or it is done on a mass scale, usually missing the more specialised audience in the critical infrastructure entirely. Therefore, the coherent spreading of cyber security awareness – probably one of the most significant factors influencing a

---

222 Marieke Klaver, Eric Luiijf, and Albert Nieuwenhuijs, The RECIPE Project: Good Practices Manual for CIP Policies. For Policy Makers in Europe, (Brussels: European Commission, 2011), http://www.tno.nl/recipereport. 10-1.

nation's overall level of cyber security – is often a lost agenda, abandoned between governmental stovepipes.

Companies involved in aspects particularly related to national cyber security – in particular ICT hardware and software companies – usually play particularly close attention to NCSS, sometimes also seeking to be involved in the drafting process itself. This can be helpful in appraising policy-makers of the actual technological state as seen from an industry perspective, and also serves the purposes of adjusting possible budgetary guidelines for major future projects. When the NCSS is directly connected to the national CIP programme this can indeed be vital step of the process. However, it is notable that very few governments make cyber software and hardware manufacturers, as well as ICT service providers, responsible for cyber security deficiencies in their products and services. Simultaneously, in more advanced nations, the cyber threat emanating from suspect hardware and software products (usually referred to as the need for 'ensuring security to the ICT supply chain') is increasingly becoming the focus of government action. What is often missing is a considered understanding of how the global internet hardware and software infrastructure, as well as the underlying operating principles such as packet routing, directly influences a nation's NCSS. As the vital components (both hardware and software) are often not only outside of the particular country's jurisdiction but (e.g., in the case of software protocols) outside *any* jurisdiction, most NCSS have few perspectives on how to engage on this issue.[223]

When it comes to communicating a 'national intent' to other countries, governments are on more familiar ground. Besides the exact language used in a NCSS, as well as the individual classification or release requirements that effectively 'set the scene', governments will of course initiate individual international actions or initiatives that underline some of messages communicated in the strategy. Within diplomatic fora, the possibilities for multi-tracked diplomacy[224] are considerable, and indeed the need to engage widely may present a challenge to traditionally-conceived foreign ministries or similar. Track 2 and Track 1.5[225] discussions are increasingly critical in building transparency between nations and increasing mutual understanding. They fulfil a real operational function – bringing senior government officials in touch not only with other government officials, but with the non-state actors that actually build and run most of what is considered cyberspace. Communicating with

---

223 For a more detailed discussion of this issue, see Section 3.

224 There are numerous definitions associated with the term 'multi-tracked diplomacy'. However, the most common and basic differentiations are between 'formal' diplomacy by diplomats (Track 1), 'informal' diplomacy by academics, experts and others (Track 2), and 'quasi-formal' diplomacy by a combination of the two actors (Track 1.5).

225 One particular Track 1.5 series of talks between China and the United States has been ongoing since 2006.

these international (or transnational) non-state actors is an activity that virtually no NCSS has yet managed to accomplish effectively.

## 2.4. POLITICAL PITFALLS, FRICTIONS AND LESSONS IDENTIFIED

There are a number of political pitfalls and frictions that policy-makers should be aware of when formulating a NSS or NCSS. In no particular order, these are:

**Adopt a 'one size fits all' strategy:** when formulating a NSS or NCSS, policy-makers may be tempted to consult other countries' existing strategies. While this may be helpful to gauge possible strategy formats and identify national interests, policy-makers should be cautious not to leverage content that is inconsistent with national requirements. To illustrate, transplanting security threats that appear in other strategies but are not germane to the country formulating the strategy may do more harm than good by diverting national resources. If there is a desire to have consistency with the strategies of neighbours and/or allies, policy-makers can mitigate the 'one size fits all' risk by prioritising perceived threats or identified policy responses. The UK, for example, prioritises its perceived security threats, identifying international terrorism, cyber attacks, international military crises, and major accidents or natural hazards as 'the four highest priority risks' over the next five years.[226]

**Neglect links with other national / international strategies:** to strengthen the relevance of a NSS (or NCSS), it should be consistent with existing and forthcoming stand-alone sub-strategies, especially those that provide greater detail on how a certain threat or challenge will be managed (e.g., a counter-terrorism strategy). Such consistency also makes it easier to identify which resources may be necessary to achieve the strategic objectives listed in a NSS. As shown in this section, establishing links across a NSS and a stand-alone sub-strategy is not always straightforward; about half the NCSS examined did not have a direct link with their states' NSS.

**Lack of an update/review mechanism:** some countries, such as the United States, have laws or other mechanisms in place to review or update existing NSS and other documents of a strategic nature. For countries that do not have such mechanisms, the formulation of a NSS or NCSS may become a one-time exercise, dependent on political will to be updated and remain valid. Thus, such strategies run a substantial risk of becoming irrelevant with the passage of time. This may be of particular concern to strategies where technological developments can quickly outdate

---

[226] UK Cabinet Office, *The National Security Strategy: A Strong Britain in an Age of Uncertainty*: 11.

portions of the strategy. To illustrate, the implications of recent developments such as cloud computing and 3D (three dimensional) printing may not be fully captured in NCSS released around 2008.

**Lack of a mid-level interagency coordination group:** the formulation of a NSS or NCSS requires input from a variety of government departments and agencies. This input can be solicited in a variety of ways, ranging from written statements to formal meetings of relevant stakeholders. In support of this process, the establishment of a mid-level, inter-agency coordination group may be useful to harmonise varying requirements across government departments. In the case of formulating a NCSS, it may also be helpful to translate technical requirements stemming from experts/users at the working level into policy-relevant language for decision-makers.

**Failing to identify critical services (NCSS):** the protection of critical infrastructures is a common requirement identified in a NCSS. As such, policy-makers have come together to identify what constitutes a critical infrastructure and which deserve special attention. In this vein, it may also be useful to go a step further and pre-identify which services are most critical for the well-being of society. Prioritising amongst these – either in a NSS or stand-alone strategy – may be beneficial in formulating a rapid response in the event of an emergency. To illustrate, the Estonian government has pre-identified 42 critical services, ranging for maintaining the electricity supply to ensuring an ice-free port of Tallinn during the winter months to facilitate the transport of goods and people.

**Lack of awareness – especially among policy-makers:** the formulation of a strategy is a means to an end. A well-developed strategy should provide policy-makers with guidance of concerning key goals, required resources, and how these could be employed most effectively. In the case of a stand-alone strategy covering a specific area, raising awareness levels among decision- and policy-makers may be particularly important to facilitate implementation. For example, concerning NCSS, strategies may suffer from weak follow-through if senior policy-makers have limited awareness of cyber issues and their implications, especially if there is a perception that the private sector should play the principal role in ensuring cyber security.

### The German National Cyber Security Council

In the German Cyber Security Strategy (2011), it was announced that a National Cyber Security Council (NCSC) would be established to help monitor the implementation of the Strategy and be able to react to new developments and threats as they occurred. The NCSC was clearly intended to be a 'political supervision' body that would not replace two other strategic and operational level government coordination bodies that were responsible for facilitating the regular day-to-day activities. Instead, this body is directly advised by the 'National Cyber Response Centre', a cyber intelligence fusion centre and cyber crisis management body, and makes decisions on addressing 'structural weakness' in Germany's national cyber security. Voting members of the NCSC include representatives of the Federal Chancellery; a State Secretary from the Federal Foreign Office; the Federal Ministries of the Interior, Defence, Economics and Technology, Justice, Finance, Education and Research; and representatives of the federal *Länder*. On specific occasions, additional ministries or agencies can be included. Business representatives are invited as associated members. Representatives from academia can be involved as required but, similar to the associate members from the private sector, they do not have any voting status or similar. Between April 2011 and September 2012 the NCSC met three times and published extracts of their deliberations online.

# 3. STRATEGIC GOALS & STAKEHOLDERS

*Alexander Klimburg, Jason Healey*

### Section 3: Principal Findings

- A national cyber security strategy (NCSS) must take into account the various stakeholder categories and their respective roles in both offensive and defensive cyber activities.
- When preparing a strategy, these stakeholders are captured within the 'Three Dimensions of NCS': the governmental, the national (societal), and the international actor groups. Accordingly, government must be able to coordinate, cooperate and collaborate (respectively) with these stakeholders.
- Besides providing challenges, the advent of cyberspace can also directly support national security goals.
- Segmentations of offensive (attack) cyber capabilities are contentious but usually address the ability to disrupt, deny access to, or destroy a system and/or to exfiltrate sensitive information from an adversary.
- Major tensions can arise between different approaches to NCS, in particular between military and civil organisations, as well as law enforcement and intelligence. Furthermore, the principal approaches of 'resilience' and 'deterrence' are often presented as being at odds with each other.
- A NCSS can be developed through a variety of processes, depending on national context and preconditions.
- A NCSS should be paired with resources and, preferably, also with quantifiable goals that can be measured. Metrics, however, are often the most difficult goal to achieve of all.
- The staffing requirements in cyber security are higher than often appreciated, due to the large number of stakeholders that need to be communicated with.

# 3.1. INTRODUCTION

This section addresses the strategic view of national cyber security (NCS), examining the basic strategic decisions that must underpin any national strategy, and identifying the national stakeholder groups with which the strategy will need to operate. Effectively, the section addresses the 'goals' and the 'means' of a national cyber security strategy (NCSS), while Section 4 will address the actual 'ways'. A NCSS needs to be orientated along not only what needs to be protected (as illustrated in Section 1) but also along the actual national security aims that need to be advanced. To achieve this goal, a number of different processes provide for the actual means, although one factor does stand out: the cooperation with other stakeholders.

Unlike most national security topics, stakeholder groups in NCS are not restricted to government entities, but include non-state and international actors as well. Indeed, the ability of a government to be able to influence NCS without taking these stakeholder groups into account is very limited. The strategic goals must, therefore, reflect the underlying basics of the cyber security domain. Consequently, this section will start with its own introduction: this includes understanding the differences between different state and non-state actor groups, absolute advantages that information and communications technology (ICT) brings to national security, and the types of offensive and defensive cyber activity. Strategic concepts such as 'deterrence' and 'resilience' are introduced as representing essential strategic choices in NCS which, however, do not need to be mutually exclusive. Moreover, the general tensions that result from strategic decisions (such as focusing on law enforcement or intelligence) are examined. The differences in policy development processes, and the choices they represent, are summarised as well. Finally, the overall engagement with stakeholder groups is explained, and a theoretical framework for segmenting these groups is introduced.

## 3.1.1. National Cyber Security Actors

'Actors' is an unpopular category to use in NCS. Defining a particular activity as, for instance, cyber crime or cyber espionage is more useful and realistic than defining the purported actor behind that activity as being a criminal or a spy. This is because accurate organisational cyber attribution is one of the most difficult tasks to accomplish in cyber security. However, it can also be misleading. From the perspective of a 'cyber warrior', cyber crime can offer the technical basis (software tools and logistic support) and cyber terrorism the social basis (personal

networks and motivation) with which to execute nationally sanctioned attacks on the computer networks of enemy groups or nations.[227]

Despite the apparent perils of classifying cyber actors in cyberspace, it is nonetheless necessary to do so, especially when trying to conceptualise the strategic environment that a NCS wishes to address. This engagement is more complex than the standard multi-stakeholder model that provides equal weighting to governments, private sector and civil society. This model obfuscates that, on the one hand, some organisations – for instance some think-tanks or other advisory groups – can actually be all three types of organisations interchangeably. On the other hand, it also ignores the fundamental importance of size and scale that the organisation is able to leverage. Finally, it largely only applies to 'good' actors, and is not necessarily helpful when dealing with, for instance, cyber crime, or 'hacktivist' gangs.

The following differentiation is not intended to replace the multi-stakeholder approach, but to be used as a conceptual aid to understanding the general 'types' of stakeholders that work in cyberspace. The challenge for government is that it usually only has experience in dealing with 'state actors', but organised non-state actors (i.e., 'large' actors) are often multinational and difficult to engage with. Even more challenging, however, are non-organised, non-state actors (i.e., 'small' actors), whose organisation, resources, fundamental outlook and particularly their sheer numbers can easily represent a crucial challenge for government to understand. Unfortunately, it is particularly this last group that contributes the most to cyber security, and also to cyber *in*security.

**State Actors:** state actors in cyberspace are, in general, the most sophisticated and well-resourced of potential cyber attackers even though some criminal cyber organisations can rival many state actors in sophistication. State actors are able to leverage large teams of well-managed programmers to design the most advanced cyber attack tools, can target them via the most sophisticated intelligence apparatus, and are able to utilise the most advanced and expensive hardware in the world. Despite media claims of how easy it would be for a single hacker to 'bring down a country'[228] with cyber attacks, in reality, the most comprehensive of cyber attacks against a nation would be a substantial operation. The simultaneous targeting of an entire country's most crucial government and critical infrastructure networks would be enormously complicated, and would likely require the type of resources only a state could leverage. A state cyber attack (especially a cyber espionage attack) is usually evident through the resources that have been leveraged to go

---

227 Klimburg, 'Mobilising Cyber Power.'

228 Cristen Conger, 'Could a single hacker crash a country's network?,' http://computer.howstuffworks.com/hacker-crash-country-network1.htm.

after a specific target, especially targets that have otherwise no obvious criminal value (e.g., the correspondence of a foreign ministry, or similar). While some of the attacks can be described as 'blatant', it can be presumed that state attacks are essentially somewhat constrained by legal norms and fear of political repercussions. For a state, cyber operations are only one of the options available to accomplish a specific political, strategic and operational goal and all of these goals can be directly addressed by a defender in various ways. On the defence, state actors have a number of advantages but also a critical and overlooked disadvantage. Governments have tremendous resources – budget, equipment and trained people – to defend against cyber attacks, but often lack agility. It can be very difficult for most government agencies to move quickly, especially if a cyber attack crosses agency lines, between different mandates, or international borders. And since most attacks affect the private sector and cross over private sector networks, governments often must rely on the private sector to undertake the actual information security activities needed to respond to an attack and restore service.

**Organised Non-State Actors:** as has been repeatedly pointed out already, cyber security is primarily a non-state affair.[229] The non-state sector is responsible for virtually all of the hardware and software used in cyber attacks, and is most often the victim of these activities. They are also probably responsible for executing most cyber espionage attacks, either for their own purposes, or to support government efforts. While the bulk of petty cyber crime is executed by small gangs or individuals, it is enabled by a much more proficient group of true cyber crime organisations which provide much of cyber crime infrastructure, and which take a large corresponding share of the profits. These can be gigantic: the single largest cyber crime organisation, the (former) Russian Business Network (RBN), was supposedly responsible for 60% of worldwide cyber crime in 2007.[230] These criminal groups can also be directly implicated in national security relevant cyber attacks. The RBN, for instance, was presumed to be at least somewhat involved in the Estonia (2007) and Georgia (2008) cyber attacks.[231] There are a number of other organised non-state actors that play an important role in cyber attacks, however. These include dedicated 'cyber militia'-type and hacker organisations that a number of governments, notably China, have been known to support.[232] They also include a virtual galaxy of security and defence contractors in North America and Europe that support the official cyber security efforts of most liberal democratic nations. All of these actors play a decisive role in cyber espionage, both as Research

---

229 See Section 1.4.1.

230 Peter Warren, 'Hunt for Russia's web criminals,' *The Guardian*, 15 November 2007.

231 Jon Swaine, 'Georgia: Russia 'conducting cyber war',' *The Telegraph*, 11 August 2008.

232 See Klimburg and Tirmaa-Klaar, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU.*

and Development (R&D) facilities developing 'cyber weapons', but also directly as agents of a nation's cyber offensive. A NCSS must pay close attention to these actors, as the problems presented by their legally often highly ambiguous role in national security is only surpassed by the actual amount of 'cyber power' that these organisations can, in fact, exert. On the defence side, large non-state actors are often vital – indeed most cyber defence can only occur with the cooperation of major software companies (such as Microsoft), security firms (such as McAfee) or telecom carriers (such as British Telecom). More agile than government but still with significant resources, these companies have been inventing new procedures to defeat attacks, with limited government assistance, such as the botnet takedowns orchestrated by Microsoft along with select non-state collaborators. At the same time, the organised non-state sector can include critical infrastructure companies, some with very poor cyber defences. These represent a threat not only to themselves, but also their wider respective national economies as a whole.

**Non-Organised Non-State Actors:** on the offense side, most of the low-level cyber crime campaigns, hacktivist activity and other minor cyber attacks are conducted by small, flat hierarchy groups, or even lone individuals. The Anonymous hacktivist network, for instance, is organised is as much as that specialised groups have emerged that are responsible for most types of cyber attacks. It is non-organised, insofar as that there is not a clear or stable hierarchy of persons that function as a command chain – normally a requirement of most definitions of an 'organisation'. Similarly, low-level cyber crime groups will only have the most basic organisation, even though outside of their particular core group they might seek to establish extensive hierarchical networks (such as via 'mules' or other part-time employees). The scope of damage that these individuals can cause directly is usually limited, but in aggregate it probably represents a significant proportion of worldwide cyber crime. These small groups are usually not responsible for the most high-value cyber crime segment, namely intellectual property theft, and thus seldom play a decisive role in a NCSS. When they are mentioned, it usually is in the more generic context of hacktivist groups, general cyber crime, and the relevant law enforcement measures. At the same time, lone actors have made a hugely positive contribution to overall cyber security, in effect, repeatedly saving the internet from itself.[233] A good NCSS will have to take the activities of these individuals into account as well. On the defence side, while small non-state actors do not have the resources that governments do, they can be very agile and have considerable technical knowledge. Moreover, these 'white hat' groups or individuals typically link large organised non-state actors and state responders and can greatly facilitate responses to cyber attacks, often faster than most governments. Smaller non-state groups, whether

[233] See Alexander Klimburg, 'Whole-of-Nation Cyber Security,' in *Inside Cyber Warfare*, ed. Jeffrey Carr (Sebastopol, CA: O'Reilly Media, 2009).

standing groups like NSP-SEC or *ad hoc* groups such as the Conficker Working Group,[234] have been extremely successful in responding to cyber attacks. Without the resources of governments, however, the non-organised non-state actors tend to lack staying power for long cyber crises: most participants are volunteers, so typically cannot sustain their engagement for a prolonged period.

### 3.1.2. National Cyber Security Advantages

In Section 1 of this publication, the wider context of NCS was explored in depth. Using the 'five dilemmas' as an example, it was illustrated that NCS would always require the right balance to be struck between the protection measures on the one hand, and the implicit and explicit costs of that protection on the other. As was said, equilibrium needs to be maintained between reaping the benefits of ICT for the country at large (in particular within an economic and individual freedom context) and protecting the country from the risks associated with ICT.

Correspondingly, the advent of 'cyber' within the national security context has often been accompanied by mostly negative connotations. To this day, the public discussion on cyber security mostly concentrates on the rising vulnerabilities and threats imposed by the steadily increasing use of ICT, rather than emphasising the benefits society has derived from it. This debate particularly emphasises the danger that our networked world is not only directly dependent on ICT, but on the supposed fragility of many societal services that need to be connected by it.[235] It is unsurprising that a security-focused view would rather concentrate on the various threats of the expanded use of ICT instead of focusing on the obvious (and less obvious) societal and economic benefits this historic development has brought us. Indeed, most NCSS try at the least to pay lip service to the importance of protecting the 'productive aspects' of ICT.[236]

A much larger facet of NCS that very seldom sees public discussion is the strategic advantages it can bring a nation purely within a national security context. These advantages are seldom explicitly discussed in public but, in all cases, the new possibilities that ICT offers national security as a whole are considerable. When considering a NCSS it is, therefore, not sufficient to purely look at the high-level

---

234 For further information on both groups, see Section 4.7.1.

235 This is traditionally understood as societal tasks 'operating at normal capacity.' Some interpretations of the 'resilience' approach to cyber defence argue that, in fact, multiple operational states are better than only delineating between a 'crisis' and a 'normal' state.

236 For a wider discussion on the productive aspects of ICT see Section 1.1.

economic and social 'Value at Risk' (VaR)[237] that needs to be addressed. Developments in ICT in general, and cyber capabilities in particular, are fundamentally having a direct impact on a number of national security relevant functions, and are greatly enhancing some of their fundamental capabilities. Because militaries are defining cyberspace as a 'domain of conflict' or an 'operational domain', this language obscures these societal and economic advantages of cyberspace, a view that can militarise policy-making. A more balanced description is that cyberspace is a domain, just like air, land, sea and space, that is generally utilised by the private sector for social and economic purposes, and in which significant conflict can occur.

What follows is an overall segmentation of this ICT-enabled security increase, loosely based around the same five mandate structure introduced in Section 1 and expanded upon in Section 4.[238]

**Military:** the current revolution in military affairs was fundamentally built upon the introduction of ICT. Ever since the total defeat of the Iraqi army in 1991, militaries worldwide have increasingly been striving to introduce various ICT-enabled capabilities to their armed forces. This includes the present paradigm of 'Network-Centric Warfare' (NCW), which is fundamentally built upon a level of communication many magnitudes greater than used by armed forces in the 1980s. The integration of these ICT enablers is often directly connected to the respective nation's overall technological development, both in terms of its ability to develop and operate some of the new NCW capabilities, be it in intelligence, logistics, or in the sensor-to-shooter cycle. Militaries can utilise cyber attack capabilities to perform local, operational-level missions (similar, in practice, to electronic warfare), or can even develop strategic-level cyber capabilities (similar in purpose to strategic air power).[239]

**Intelligence & Covert Operations:** the intelligence community has long understood the value of cyber espionage. As far back the 1980s it was said that, 'espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations [...] insulated from risks of internationally embarrassing incidents.'[240]

---

237 There are a number of high-level papers that use the term 'Value at Risk' within a cyber context. See, for instance, John Dowdy, 'The Cybersecurity Threat to U.S. Growth and Prosperity,' in *Securing Cyberspace: A New Domain for National Security*, ed. Nicholas Burns and Jonathon Price (Washington, DC: Brookings Institution Press, 2012).

238 The lack of a complete overlap between the 'five mandates' and the above segmentation is not accidental. While the five mandates cover different facets of NCS, overall the benefits of ICT to cyber security accrue differently.

239 That is, cyber capabilities both enable traditional military forces to do their job better through interconnectedness (as illustrated by the US information superiority over Iraq in the First Gulf War), but might also be used as a form of offensive attack in its own right.

240 Cliff Stoll, 'Stalking the Wily Hacker,' Communications of the ACM, Volume 31, Issue 5, May 1988.

Foreign intelligence gathering has been fundamentally revolutionised through cyber capabilities. It is possible to say that cyber capabilities have had a greater impact in this field than in any other security area. In essence, three trends are especially obvious: the extension of effective 'Signal Intelligence' (SIGINT) capabilities through direct application of cyber means (e.g., cyber espionage through software and hardware); the ability to recruit and manage 'Human Intelligence' (HUMINT) resources via cyberspace, and the greatly heightened ability to integrate various sources of 'deep data' and other intelligence into a common intelligence picture, including 'Open Source Intelligence' (OSINT) as well as information from friends and partners. Moreover, some countries may include the ability to wage 'information warfare'[241] against their adversaries in a form of covert operation, resident within the intelligence and not the military structures. Internal security is probably one of the most sensitive issues for democracies. It is, however, far from certain if there has been a net increase in domestic intelligence capabilities and, considering the additional challenges that internal security services face due to the advent of ICT (e.g., due to criminal use of encryption). On the other hand, many countries have not published the extent of their true surveillance capabilities on domestic and foreign networks.

**Law Enforcement:** the considerable efficiency increases in traditional policing due to ICT have probably only been partially offset by the advent of entire new forms of criminal activity.[242] Much media attention has focused on the deployment of 'Closed-Circuit Television' (CCTV) and similar surveillance technology, but the ability to increase the mobility of through information gathering, analysis and dissemination tools is probably equally as important. Cyber crime represents its own significant challenge to the economic and social basis of a country and is likely to increase in the future. Equally, many countries will harbour international cyber crime infrastructure without law enforcement being aware of it.

**Diplomacy & 'Soft Power':** the ability to define international norms and standards relevant to international behaviour in cyberspace represents its own form of 'soft power.'[243] Even small countries can exert particular influence in this area if they are seen as being credible partners due to their overall level of cyber security development or ICT literacy.[244] Other countries may represent particular legal facets of relevance to cyber (e.g., focusing on human rights or an overall 'internet Freedom' agenda). It is certainly possible to leverage overall issues in diplomatic

241 For various definitions of Information Warfare see Section 1.

242 For a list of trends of ICT in policing see Sebastian Denef et al., ICT Trends in European Policing, (Sankt Augustin: Fraunhofer-Institut für Angewandte Informationstechnik FIT, 2011), http://www.fit.fraunhofer.de/content/dam/fit/de/documents/composite_d41.pdf.

243 See Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011). 81-109.

244 One notable example being Estonia, but also Finland and Sweden can be named here.

cyber security forums to further other political, economic or indeed security agendas.

**Emergency Services:** this vast category includes all ICT that facilitates the work of the emergency services besides law enforcement. This can range from improved communication and analysis tools for first-responders, national crisis management and continuity of government systems to comprehensive critical infrastructure protection programmes and their associated information exchanges. Overall, these systems deliver a greatly increased level of security for specific risks.

The first three points of the above list – the military and intelligence capability gains because of 'cyber' – are very seldom discussed or even touched upon in public. What exactly these capabilities are can sometimes be inferred from various secondary sources or geopolitical events and has been speculated on elsewhere.[245] In particular, in countries with a highly engaged foreign policy, these capability increases are very significant, and have significantly shaped the entire international security paradigm. Information warfare, or cyber power[246] has the potential to be a decisive form of national power, able to inflict strategic blows on the adversary without ever having to resort to kinetic means. It is even possible to wage a 'war' without the adversary ever knowing that a war has been started.

As was remarked upon in Section 1.4, there is a clear difference between those advanced cyber nations that have a high level of ambition in integrating cyber security within their overall international policy and foreign posture, and those who address NCS more as an internal security task. In essence, some nations will seek to purely mitigate against cyber risks, while other nations might seek to exploit those same risks. Overall, however, both types of nations will first need to work within the basic technical realities of attack and defence within cyberspace, and decide which type of strategic concept would best fit their needs.

### 3.1.3. Offensive Actions in Cyber

One of the most fundamental dichotomies in national cyber policy is between cyber offence and cyber defence, more often generally framed as 'attack' and 'defence'. The goals of cyber offensive capabilities vary. Non-state actors will attack in order to steal monetisable information (such as credit card numbers), or to increase their status with their peers. State actors may choose to use offensive cyber capabilities to spy on their neighbours or steal their industrial secrets, to disrupt attacks against

---

245 See, for instance, Klimburg and Tirmaa-Klaar, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU.*

246 See Klimburg, 'The Whole of Nation in Cyberpower.'

themselves (often known as 'active defence'), employ cyber weapons in lieu of more traditional kinetic weapons during an armed conflict, or as covert actions against adversaries during a strained peace. Put otherwise, each of the five mandates of national cyber security will have their own relevant definitions of cyber attack, and each definition will need to be accounted for in a comprehensive strategy.

The term 'cyber attack' is not internationally defined – there are substantial differences between, for instance, the US definition and most others.[247] Furthermore, there may be significant differences of definition even within a single country, in particular across the different NCS mandates.[248] The most general definition of a cyber attack is a malicious premeditated attempt to disrupt the confidentiality, integrity or availability of information residing on computers or computer networks.[249] In order of severity, these attacks include the adversary seeing information they are not supposed to (e.g., spying), disrupting the legitimate use of that information to others (e.g., blocking a transmission, or shutting down a service), or changing information without authority (which can range from manipulating personal data to interfering with the control systems of industrial facility, with catastrophic results).[250] This segmentation has also be used in studies of (military relevant)[251] cyber attacks and has been quoted by senior defence officials.[252] The segmentation is not only a result of the 'effects' accomplished by a cyber attack but also of the extent of how directly the cyber attack was responsible for those effects. Within this context, three levels of severity can be distinguished:

**Background Noise:** the first level has been called 'network wars', or also 'system administrator versus system administrator.' This includes mobile malicious logic, trojan attacks, basic phishing attempts, common exploits, and the sum total of attacks that many organisations are constantly facing – often simply referred to as the 'background noise' of information security. Some governments have defined this as the Computer Network Exploitation (CNE) level, implying that most conventional cyber crime and all of cyber espionage is limited to this level, regardless of severity,

---

247 See Section 1.2.4.

248 To give a hypothetical example, a counter-cyber crime definition might read: 'an act of trespass on a personal computer system represents a cyber attack' while a military definition might read 'a cyber attack is a hostile military act conducted through cyberspace.'

249 See Kevin O'Shea, 'Cyber Attack Investigative Tools and Technologies,' in *HTCIA* (Hanover, NH: Dartmouth College, 2003).

250 It is important to avoid the general implication here that, in all cases, 'confidentiality' is ranked beneath 'availability' which is ranked beneath 'integrity'. In fact, every system will prioritise C-I-A based on its own unique requirements.

251 Based on a study by the US Air Force Science Advisory Board (AF-SAB), quoted from Raphael S. Mudge and Scott Lingley, 'Cyber and Air Joint Effects Demonstration (CAAJED),' (AFRL/RIGB, 2008), 1-2 and 8.

252 See, for instance, John D. Banusiewicz, 'Lynn Outlines New Cybersecurity Effort,' *American Forces Press Service*, 16 June 2011.

unless it modifies or destroys data. The (by no means uncontroversial) assertion is that all of these attacks should be considered 'routine', and can be lowered to a reasonable level by proper cyber security procedures. On the other hand, many nations would not agree with the view that CNE comprises only the lowest level of cyber attack severity. In some cases, it can be argued, a successful CNE attack could have catastrophic implications for national security. Further, a CNE attack would often be a prerequisite for a 'kinetic equivalent' cyber attack. Detractors would therefore argue that cyber espionage should not be treated as a 'gentlemen's misdemeanour', as the technical nature of some cyber espionage attacks could be misconstrued as a more serious attack, thus leading the way to a loss of escalation control between the parties.

**Cyber Adjunct to Kinetic Combat:** this attack is one where the intent is to achieve a 'kinetic effect' through a cyber attack (e.g., the denial of function of an IT-based system, such as radar or communications facility) to facilitate a conventional attack on a secondary target. The use of malicious logic to disable an air defence network in context of a wider air strike is an example of such an attack.[253] However, under specific circumstances (such as a simultaneous ground invasion) this could equally apply to a particularly devastating distributed denial of service (DDoS) attack.[254] The underlying notion is that a cyber attack can rise to the level of a physical attack: a 'use of force' in legal terms. This interpretation implies that the actual damage is not necessarily caused by the cyber attack itself: rather, the cyber attack simply enables the actual destruction to occur with other means.

**Malicious Manipulation of Data:** unlike in the previous example, here the cyber attack itself is the actual destructive agent. By directly changing the programmed parameters of a system or database, it can cause wide-scale death or destruction. One view is that these attacks are 'the ones to be feared, they are covert, they are planned, they are orchestrated, and they can cause widespread havoc and disruption without the victims realising their problems are cyber related.'[255] Essentially, these attacks refer to both invisible and wide scale manipulations of systems with potentially obvious catastrophic results (e.g., for a gas pipeline, a power generator, or a transportation facility)[256] or a less visible but equally dangerous manipulation

---

253 Such a cyber attack against an air defence system is said to have occurred within the context of the Israeli Operation ORCHARD against a purported Syrian nuclear facility in 2007 (see Thomas Rid, 'Cyber War Will Not Take Place,' *The Journal of Strategic Studies* 35, no. 1 (2012): 16-7.).

254 The term 'distributed denial of service' refers to an attack where an individual computer is flooded with information from many other computers, forcing it to slow, shut-down or malfunction.

255 Mudge and Lingley, 'Cyber and Air Joint Effects Demonstration (CAAJED),' 1.

256 Catastrophic cyber attacks are rumored to have occurred already on a Soviet gas pipeline in the early 1980s (see Klimburg, 'Mobilising Cyber Power.'), and has been academically tested in the AURORA experiment in 2008 (Tom Gjelten, 'Stuxnet Raises 'Blowback' Risk In Cyberwar,' *npr*, 2 November 2011.).

of data to degrade the target over time (e.g., at a nuclear enrichment facility[257] or in personal medical databases). In the most serious of cases, it is possible that such attacks could amount to an 'armed attack'.

From one military perspective, a serious cyber attack probably only refers to the last two examples: when data is actually denied or manipulated/destroyed. Under international law (*ius ad bellum*) it is possible that these attacks could amount to a use of force, or an armed assault, if physical damage or loss of life results.[258] Ultimately, the actual effects of an attack are more important than whatever segmentation is chosen or indeed the actual intent of the attack itself – a 'manipulation of information' attack that has no significant results could hardly constitute a *casus belli.* On the other hand, it is probably quite relevant to distinguish a cyber attack as either a facilitator, or the actual destructive agent, as the above segmentation tries to do.

The above model of cyber attack has one particular implication: the level of a cyber attack is not a reflection of the intent of the attacker, but rather the measure of the failure of the defender. Consequently, in cyber security, the onus may be shifting towards the responsibility of the defender to adequately secure their systems. Put differently: if a 15-year-old teenage hacker tries to execute a devastating malicious manipulation of data attack on a critical infrastructure 'just for laughs', and the company in question has clearly failed to provide for a minimum level of cyber protection, then the possibility of the company being culpable in facilitating the attacks can be raised. Recent European Parliament legislative proposals indicate that there is increasing support for expanding the duty of care concept to include cyber attacks.[259]

A different segmentation could be to look at the relevance of a particular cyber attack for one of the five NCS mandates. This is segmentation based on the kind of activity undertaken by the attacker, either to steal information (confidentiality attack) or disrupt systems, or the information on or passing through those systems (integrity or availability attacks). The national impact of these attacks can be either low (being a crisis for a particular person or company but not a national issue) or high (which gets escalated to elected officials as a national security issue).

---

257 The 'Stuxnet' cyber attack on the Iranian enrichment facilities was especially programmed to slowly degrade the centrifuges over time, rather than catastrophically destroy them outright.

258 For a discussion on what could constitute 'use of force' within a cyber operations context, see Rule 11 in the Michael N. Schmitt, gen. ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, forthcoming 2013).

259 For instance, this view is partially reflected in points 11-12 of the preamble of the 2012 Revision of the 2005/222 JHA European Directive on attacks against information systems.

| TYPE OF ACTIVITY | NATIONAL LEVEL IMPACT: Low | NATIONAL LEVEL IMPACT: High |
|---|---|---|
| Information Theft | Counter Cyber Crime | Intelligence/CI |
| Information Disruption | Counter Cyber Crime and/or CIP – Nat'l Crisis Mgmt | CIP – Nat'l Crisis Mgmt and/or Military Cyber |

**Figure 2:** Parsing Cyber Offense

Obviously, a cyber strategy that focuses most on national security should focus most on the right-most column. If protection of citizens and companies is the focus, then the left-most column may be more important, as low-impact attacks form the vast bulk of cyber incidents.

From one military perspective, a serious cyber attack only refers to the bottom right quadrant: when data or systems are actually denied or destroyed on a large enough scale to be nationally significant. Under the Law of Armed Conflict it is possible that these attacks could amount to a use of force, or an armed assault, if physical damage or loss of life results.

### 3.1.4. Defensive Actions in Cyber

For decades, it has been far easier to attack than to defend. Attackers can hide their identity with impunity, computers and networks are complex and difficult to adequately defend, and weak international governance has allowed some nations to become sanctuaries for insecure computers and nests of criminal attackers. Therefore, all NCSS have at their core a 'defensive' mission.

Typically, defensive actions are taken entirely within one's own networks but there are exceptions. Law enforcement organisations have authority to arrest perpetrators in response to cyber intrusions while militaries might retaliate with

cyber attacks or even use lethal force for a particularly disruptive cyber attack. In essence, cyber defence is often broken into four actions:[260]

**Protect:** this action is usually defined as 'getting the bare basics right'. This means having up to date antivirus software(s) for the most primitive threats, having appropriately configured firewalls, and ensuring that all applications are constantly updated. Colloquially, actions to protect information systems are sometimes considered as 'information assurance', a more extensive business process-orientated paradigm than computer network defence (CND). The concept of information assurance goes beyond CND in that it treats all information – irrespective of the medium upon which it is stored – according to various protection principles. This is helpful in as far as the data not stored in a computer (for instance stored on paper, or indeed in a conversation) can be vital in enabling an attack on a secure computer network. A 'protection' system that only takes into account technical measures and ignores the business processes that they are supposed to support, will fail in its purpose.

**Detect:** in this phase it is already presumed that something untoward is happening on the system, and depends on automated systems such as Intrusion Detection Systems (IDS) as well as numerous more intrusive technologies such as Deep Packet Inspection (DPI) to find the evidence, usually in the form of unauthorised data leaving the system. This is paired with the necessity of 'hunting on one's own networks' to proactively (and manually) root around possible file locations where a hacker may have established access.

**Respond:** once a breach has been discovered it is time to respond. This can take a great many different forms. On the simplest level, this can mean just deleting a file or closing a firewall port. But at the more advanced level this can mean shutting down an entire network, replacing hardware and rebooting from the backups, if these themselves are not contaminated. Following a cyber attack on the Swiss Foreign Ministry in 2009, large parts of the ministry system (including e-mail) had to be shut off for a number of days.[261] Even more dramatic are potential situations involving possible nation-wide cyber attacks which, in theory, could require disconnecting internet connections entirely. Within most operational contexts, this responsibility will reside with the national or governmental Computer Emergency

---

260 See US Nuclear Regulatory Commission, *Regulatory Guide 5.71. Cyber Security Programs for Nuclear Facilities* (Washington, DC: US Nuclear Regulatory Commission, 2010). There are other variations of this model. The FIRST/CSIRT community talks of 'Protect, Detect, Respond and Sustain.' See FIRST, 'Best Practices Contest 2008: Project,' http://www.first.org/conference/2008/contest.html. Others, however, add 'defend' to this category as well, usually in the context of advocating 'active defence.' (See NSA, *Defense In Depth. A practical strategy for achieving Information Assurance in today's highly networked environments. USA.* http://www.nsa.gov/ia/_files/support/defenseindepth.pdf).

261 Christopher von Eitzen, 'Online attacks on Swiss foreign ministry,' *The H Security*, 27 October 2009.

Response Team (CERT).[262] A CERT has been defined as 'a team that coordinates and supports the response to security incidents [any adverse event which compromises some aspect of computer or network security] that involve sites within a defined constituency [the group of users, sites, networks or organizations served by the team].'[263]

**Recover:** the process of recovery starts during the actual mitigation of the cyber attack. To ensure that the end-user suffers as little disruption as possible, so-called Business Continuity Management (BCM) systems depend on external and spare resources, or altogether different means, to limit the downtime to the system. Similarly, all systems require a set of backups or Disaster Recovery (DR) systems in order to replace corrupt or lost data. The infrastructure requirements for this recover stage are often immense, with spare data centres and bunkered repositories for information being the norm for most government systems.

More recently, the nature of defence has been shifting. While 'passive' defence is still considered the priority, very influential voices – including the former second most senior responsible military commander in the United States – have been clamouring for counter cyber attacks. This trend towards 'active defence', to use some types of offensive capabilities to disrupt incoming attacks, has become US Department of Defense (DoD) policy.[264] While some European NATO nations have provided indications that they may consider the general approach of 'active defence' a valid one, it is not clear if all the ramifications of these types of automated counter-attacks are understood, and if the threat of inadvertent and unintended escalation has been fully addressed. Still, the attractions of active defence are obvious: with the securing of networks being a seemingly endlessly expensive task, active defence seems to provide a cheaper method to defend – or to 'deter' – against potential cyber attacks. This is an influential argument but is still unproven.

---

262 A CERT is a specific organisation designed to address information security threats. In general, it is defined by five tasks: '1. Provide a reliable, trusted, 24-hour, single point of contact for emergencies; 2. Facilitate communication among experts working to solve security problems; 3. Serve as a central point for identifying and correcting vulnerabilities in computer systems; 4. Maintain close ties with research activities and conduct research to improve the security of existing systems; 5. Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers' (Carnegie Mellon University, 'About Us,' CERT, http://www.cert.org/meet_cert.). Also see Section 4.2.1.

263 IETF RFC 2350, 'Expectations for Computer Security Incident Response,' June 1998, http://tools.ietf.org/html/rfc2350.

264 US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*.

### 3.1.5. Collective Cyber Defence

In essence, all real cyber defence is 'collective'.[265] Short of disconnecting from the internet (and not even that can be sufficient), organisations are nearly always reliant upon other organisations, Internet Service Providers (ISPs) or countries to help them stop a significant cyber attack. Within NCS, however, the notion of 'collective cyber defence' is increasingly having a more specific international connotation. While no standard definitions exist, collective cyber defence can be said to be 'the operational cooperation of various (international) actors to defeat specific cyber attacks directed against one or more of the respective actors'. There are a number of operational methods that can be utilised for collective cyber defence. These can range from the simply sharing and pooling of intelligence resources, human resources or even actual communication infrastructure. States supporting another country in collective cyber defence can also physically interfere or manipulate internet traffic transiting through their respective country, or ultimately use their own deployed cyber capabilities to offensively engage in cyber operations against the attacker. Essentially, collective cyber defence can not only play a role with the 'detect' and 'respond' phase of cyber defence, but could theoretically involve offensive and active-defence operations as well.

Collective cyber defence is overwhelmingly built upon individual and organisational trust and this trust can even supersede traditional alliance structures. The United States Cyber Storm III exercise included a number of countries as active participants but the countries were individually invited. The NATO Cyber Coalition, which also conducts regular large-scale collective cyber defence exercises,[266] is not only composed of Alliance members. Indeed, in recent years a number of Organisation for Economic Co-operation and Development (OECD) countries have initiated direct bilateral cyber defence cooperation agreements with each other. While often these discussions focus along crisis-prevention information sharing tasks, a real subtext is the need to create existing institutional and personal relationships that can be activated in a crisis to enable true collective cyber defence. No NCS strategy should underestimate the importance of these relationships.

## 3.2. STRATEGIC CONCEPTS: BALANCING DEFENSIVE AND OFFENSIVE

A NCSS can be judged on the basis of whether it has made a nation's cyberspace more secure from attack or not. Optimally, this would involve raising the barriers

---

[265] For a discussion on NATO cyber initiatives see Section 5.3.

[266] James G. Stavridis and Elton C. Parker, 'Sailing the Cyber Sea,' *JFQ* 2, no. 65 (2012).

to attack and lowering the limitations to the defence to such an extent that most attacks, both criminal and state, would simply not be cost effective.

The important decision is the balance of how much of a nation's resources should be directed towards defence or offense. While morally it would appear there is a clear choice which cyber security aspect a nation should favour, financially the choice is not nearly as clear. Cyber defence is enormously expensive; it involves massive investment of financial and human resources to adapt organisations, technology and processes (and even basic human behaviour traits) to comply with proper information security procedures. In the late 1990s, the US DoD made defence the clear priority, judging that their traditional military power could coerce any likely adversaries without the use of offensive cyber capabilities. But if the DoD's own cyber systems were disrupted, all of those traditional military forces could be left deaf and blind.[267]

Today, however, few nations believe that a complete cyber defence is possible – no ICT system is forever completely immune to a cyber attack. It is, therefore, unsurprising that there have always been voices which have stated that the strongest protection against cyber attack was the threat of counter-attack, in other words: 'deterrence'. Deterrence theory is increasingly countered by those who believe that deterrence cannot work due to the anonymous nature of most cyber attacks. They argue that it is more important to design operational systems that can withstand serious technical disruptions, or can change their standard of operations to adapt to the new situation. This approach has often been referred to as 'resilience'.

Both these approaches are not directly in opposition to each other. For instance, deterrence advocates will often insist that resilience is merely part of a good deterrence strategy. Also, it would seem that deterrence has a much stronger role in advanced cyber nations, in particular, in the United States, while smaller nations will always have to be more orientated towards 'resilience'. Both strategies, however, are relevant for countries of various capabilities and, most importantly, have one common denominator: they depend on greatly increased cooperation between various actors to achieve their goals.

### 3.2.1. 'Deterrence': Cost Imposed

Deterrence can be defined as '[d]eterring or preventing by fear.'[268] The concept of deterrence is not particularly new. As an instrument of classical diplomacy, the

---

267 Jason Healey et al., Lessons From Our Cyber Past: The First Military Cyber Units [Transcript], (Washington, DC: Atlantic Council, 2012), http://www.acus.org/event/lessons-our-cyber-past-first-military-cyber-units/transcript.

268 Deterrence, *Oxford English Dictionary Online* (Oxford University Press, 2012).

threat of war has ever since been applied when states were trying to prevent others from behaving in a way that could potentially harm their own interests. However, deterrence theory, as it emerged during the early years of the Cold War, was remarkably different. While in the pre-Cold War era, the threat of using force was repeatedly carried out by the parties involved, in the era of nuclear weapons, deterrence 'must be *absolutely* effective, allowing for no breakdowns whatever. The sanction is, to say the least, not designed for repeat action. One use of it will be [one] fatally too many.'[269] However, while it is widely accepted today that 'nuclear weapons had become a source of intolerable risk,'[270] deterrence through retaliation is still a timely policy instrument under study.[271] More recently, deterrence strategy has also been linked to 'cyber'. In this context, cyber deterrence was defined as the 'capability in cyberspace to do unto others what others may want to do unto us.'[272]

Cyber deterrence is sometimes based upon so called cross domain response abilities.[273] For instance, this can include the ability to retaliate against a cyber attack in a domain of conflict[274] other than cyber, such as when the United States declares, '[w]hen warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.'[275] This means that retaliation has many forms, including economic or diplomatic means. Within this context, smaller nations may also be able to deter larger aggressors with non-cyber means, even if only within the limited remit of international trade and diplomacy.

Deterrence can also be built on responses solely within the cyber domain. One excellent example is from General Cartwright, formerly the second most senior military officer on cyber security in the United States, who said, '[w]e've got to talk about our offensive capabilities and train to them; to make them credible so that people know there's a penalty to this.'[276] More recently, adherents of the deterrence model have received additional support from the (mostly US) trend towards active defence. Here, there is a more direct cyber response to quickly disrupt inbound attacks. The goal is not to inflict a direct penalty on the attackers but to ensure that their attacks are fruitless.

---

269 Bernard Brodie, 'The Anatomy of Deterrence,' *World Politics* 11, no. 2 (1959): 175.

270 The Economist, 'The Growing Appeal of Zero. Banning the bomb will be hard, but not impossible,' *The Economist*, 16 June 2011.

271 See, for instance, Amir Lupovici, 'The Emerging Fourth Wave of Deterrence Theory – Toward a New Research Agenda,' *International Studies Quarterly* 54, no. 3 (2010).

272 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Pittsburgh: RAND Corporation, 2009). 27.

273 John C. Mallery, 'Models of Escalation and Desescalation in Cyber Conflict,' in *Workshop on Cyber Security and Global Affairs* (Budapest: International Cyber Center at GMU and CERT-Hungary, 2011).

274 These domains are known, for instance, as Diplomatic, Informational, Military, Economic (DIME).

275 White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*: 14.

276 Andrea Shalal-Esa, 'Ex-U.S. general urges frank talk on cyber weapons,' *Reuters*, 6 November 2011.

The cyber deterrence model has, in theory, an obvious cost effective angle to it: overall defence-by-deterrence is thought to be cheaper than 'comprehensive hardening' of one's systems from all possible attacks.[277] However, deterrence probably works best against the most damaging attacks, those from nations which are equivalent to a traditional military attack. The United States, for instance, spends the vast majority of its cyber budget on defensive measures, despite a clear deterrence policy, only strengthened by the recent emphasis of active defence. Also, there are considerable problems with other aspects of this strategy, in particular with attribution, but also with strategic messaging and communication of abilities. Irrespective of potential classified advances in technology, it is highly unlikely that cyber attribution will ever rise to anything like the level of attribution given for, as an example, an inter-continental ballistic missile (ICBM) attack.[278] That poses the question: how much attribution is enough? Would, for instance, a 50% cyber attack attribution be sufficient in a strategic conflict environment? Furthermore, deterrence requires that robust offensive cyber capabilities not only be discreetly available, but that the potential adversary also be informed that these capabilities exist.

Though today's crimes and nuisance disruptions may be difficult to attribute, this is likely to be a very thin veil if the attacks significantly disrupt economies, actually destroy property, or cause casualties. In the end, attribution of large scale disruptive attacks may be decided not by technical attribution but which nation seems most responsible, such as by being the source of the attacks, encouraging or directing its citizens to attack, or repeatedly ignoring requests to cease apparent or tacit support of the attacks.

Cyber deterrence as a concept is particularly complicated as, similar to the term 'cyber attack', it is often applied indiscriminately across the different NCS mandates. Cyber criminals, spies and foreign militaries generally need to be deterred in different, and in sometimes contradictory, ways.

### 3.2.2. 'Resilience': Benefit Denied

Instead of threatening to retaliate in the case of aggression, an alternative view of NCS builds upon the idea of system stability, or resilience. 'We are in the midst of a cyber war of words,' former US Cyber Coordinator Howard Schmidt said: 'Let's quit

---

277 Libicki, *Cyberdeterrence and Cyberwar*: 33.

278 Within NORAD (North American Air Defence), a 'dual phenomenology' system is employed for missile attack-detection. This means that two separate sensor systems (e.g., radar, TELINT, IMAGINT, etc.) have to independently register an attack before that attack is confirmed as such. Therefore, 'attribution' is very high indeed, above 98% certainty.

pointing fingers and start cleaning up the infrastructure.'[279] This quote illustrates better than most the central two tenets of the resilience approach to NCS. Firstly, they demonstrate that the vast majority of cyber attacks are only possible due to the wide scale failure to apply basic cyber security principles. Secondly, they make it clear that cyber attacker 'attribution is very difficult,'[280] if not even impossible. Therefore, any model based on pursuing the enemy actor in cyberspace is likely to fail.

Consequently, the best defence is to raise the costs to the attacker by making the systems more secure and resilient, in effect: to 'deter through denial'[281] (against both cyber espionage and direct cyber attack) or by 'raising the work-factor'[282] for the attacker. This approach is particularly attractive to less advanced cyber nations, as their technical abilities as well as geopolitical weight are probably more limited in any case. However, it is generally also seen as an overall trend in security thought: namely, the drive towards 'resilience' in many aspects of overall security policy.

Historically, the concept of resilience dates back to the early 1970s, and was first applied in studies on ecological systems.[283] In this context, two contrasting aspects of resilience have been identified: one that concentrates on stability near an equilibrium steady state ('engineering resilience'),[284] and another one that accepts that system stability can also be maintained by changing into an alternative equilibrium ('ecological equilibrium'). While the first aspect of resilience focuses on maintaining *efficiency* of function, the second one concentrates on maintaining *existence* of function.[285]

---

279 Glenn Chapman, 'Too Much Hysteria Over Cyber Attacks,' *Discovery News*, 16 February 2011.

280 Tom Espiner, 'US cyber-tsar: Tackle jailbroken iPhones,' *ZDNet*, 24 March 2012.

281 Defense System Staff, 'Overlapping defense essential to deter cyberattacks: Panel members,' *Defense Systems*, 8 November 2011.

282 See, for instance, John C. Mallery, 'International Data Exchange And A Trustworthy Host: Focal Areas For International Collaboration In Research And Education,' in *Digital ecosystems network and information security and how international cooperation can provide mutual benefits* (Brussels: BIC, 2011).

283 See Crawford S. Holling, 'Resilience and Stability of Ecological Systems,' (Vancouver: Institute of Resource Ecology, 1973). The 'ecological resilience' view is slightly different from the 'engineering resilience' view. Ecological resilience is 'the amount of resistance to change to shift a system from one stable state into another stable state.' In this context there are many 'stable operating states', and some of these may be required for the long-term good of the system. The example often given is the need to have small fires in a forest in order to prevent a larger fire.

284 Resilience can be defined as 'the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions' (UNISDR, 'Terminology,' http://www.unisdr.org/we/inform/terminology.).

285 Crawford S. Holling, 'Engineering Resilience versus Ecological Resilience,' in *Engineering Within Ecological Constraints*, ed. Peter C. Schulze (Washington, DC: 1996).

The resilience model has an obvious logical appeal: the ability to manage cyber security by concentrating a nation's efforts internally (e.g., focusing on internal processes and products) rather than trying to externally influence nations and other actor groups. It also seems to be a 'quick win': all that needs to be done would be to 'clean up' the infrastructure. However, the problem is that this cleaning is certainly not a simple task, and can be very expensive. Indeed, it can even cost more than the actual damage of the attacks themselves. A (controversial) 2012 UK study on cyber crime even claimed that cyber security 'countermeasures' cost four times as much as the actual damage caused by cyber crime.[286] Secondly, there are technical aspects that make cyberspace inherently insecure and are virtually impossible to completely 'fix' (in particular the nature of protocol and protocol suits such as BGP, DNS and SCADA[287]). Thirdly, the notion that attacks will decrease with the increased work load for the attacker is theoretical. In fact, it is perfectly possible that more serious targeted attacks (e.g., those most relevant for national security) will simply become more sophisticated themselves. Finally, besides the investment in material resources, 'true' resilience demands a major change in organisational thinking. This is often the most costly change element of them all.

## 3.3. TWO TENSIONS OF NATIONAL CYBER SECURITY

Fundamentally, there are two axes along which a nation's NCS can be concentrated: military and civilian, as well as intelligence and law enforcement. The focus of a nation's NCS will depend on the specific local conditions, as well as the exact interpretations of the word NCS, for instance, if it includes offensive capabilities as well. Fundamentally, it is possible to say that both of these axes are often orthogonally different in goals, organisation and operational culture. This does not mean that they are completely mutually exclusive – often a substantial grey area will exist, e.g., with domestic intelligence services. However, often the central tenets of the respective groups are different to reconcile.

### 3.3.1. Military vs. Civilian Approaches

In some OECD countries there has been a heated debate as to the role of the military in NCS. Largely, the question is one of principle: in the United States, for instance, the role of the military in internal security issues is closely circumscribed

---

286 Detica, *The Cost of Cyber Crime. A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.*

287 Border Gateway Protocol, Domain Name System, and Supervisory Control and Data Acquisition, respectively.

by the US constitution. It is also a question of roles, such as where does the primary relevant intelligence[288] body reside, or what role does the military have in other relevant national crisis management tasks. From a similar perspective, the role of the military in Critical Infrastructure Protection (CIP) is often very contentious.

Overall there are quite different approaches to integrating the military in NCS. In the UK and Germany, for instance, the military plays a very small role (if any) in CIP, and has a very much subordinate role within the larger context of NCS. In France the situation is reversed: while the interior ministry retains control of the actual political national crisis management structure, the defining actors in NCS (as well as the use of cyber elements abroad) are all subordinate to the Secretariat-General for National Defence and Security (SGDSN[289]). In the United States, the role of the DoD, in the wider CIP programme was limited until 2010,[290] although the DoD has always leveraged the most cyber security resources, both in defence and in attack. Since 2010 there has been repeated attempts to bring the DoD (and in particular the NSA) closer into the national CIP programme,[291] with marginal success. In Europe, nations associated with the 'total defence' concept often have similar approaches. In Switzerland, for instance, the main NCS organisation, the Reporting and Analysis Centre for Information Assurance (MELANI), is situated within a civilian ministry but the organisation depends on its ability to mobilise resources from the military and intelligence community.

### 3.3.2. The Law Enforcement vs. Intelligence Community Approaches

It is important to understand that the interests of the intelligence/counter-intelligence[292] community (IC) are very often in direct opposition to the interests of law enforcement (LE) in general. Both the intelligence/counter-intelligence and counter cyber crime mandates are clearly separate. Simple phishing attacks, for instance, are not normally a matter for the IC. Nonetheless, some attacks, in particular those involving intellectual property or those which are conducted with a high level of sophistication, such as most Advanced Persistent Threats (APT), will

---

288 Exactly which intelligence body is the most relevant is a separate subject and depends on the relative focus of the nation in question. In some countries the ability to do signal intelligence and collection abroad will be a priority, while in others the role will be defined more in terms of traditional counter-intelligence.

289 In French: *Secrétariat général de la défense et de la sécurité nationale*.

290 US Department of Homeland Security, *Joint Statement by Secretary of Defense Robert Gates and Secretary of Homeland Security Janet Napolitano on Enhancing Coordination to Secure America's Cyber Networks* (Washington, DC 2010).

291 Known as Critical Infrastructures and Key Resources (CIKR) Programme.

292 In US parlance this is often described as 'national security'.

often involve both the IC and LE, especially where their jurisdictions overlap in supporting the CIP mandate. Any attempt at conceiving a NCSS needs to take into account that the two parts of government most operationally involved in protecting against cyber attacks have fundamentally different world views:

**Openness:** intelligence agencies will go to great lengths to prevent revealing the means and methods of intelligence collection. A result of this is that the over-classification of cyber intelligence is endemic in many countries,[293] and is generally considered to be one of the most significant challenges in information sharing,[294] including from IC to LE bodies.[295] LE, in contrast, will mobilise all means of cyber intelligence, much of which will be commercial or open source, and distribute it widely.

**Motivation:** while LE aims to apprehend and prosecute a culprit, the IC will often seek to observe and exploit that actor's action for a later advantage. While LE can also be said to have a *prima facie* interest in an attacker's motivation, intelligence agencies will assign much more weight to the actor's motivation and background. Discerning intent has always been one of the most important roles for the IC.

**Offensive:** LE will very seldom seek to conduct a Computer Network Attack (CNA) or a Computer Network Exploitation (CNE).[296] Therefore, they have no vested interest in keeping a discovered attack method or exploit secret. Instead, LE will often see it as their direct (organisational) interest to distribute information of the attack to as many parties as possible. In an extreme case it might even be to the initial victim's disadvantage to have the information of their attack shared, but might be judged by LE as being in the interest of public safety. In contrast, some intelligence agencies might actively want to discourage information of an attack tool or method from being shared, either to be able to entrap further attacks or indeed to be able to carry out their own attacks.

**Sharing:** information exchange is sometimes viewed as the most important component in NCS, especially when it occurs between the private sector and the government. In some cases the information can be particularly sensitive –

---

293 For the case of the US see Sean Reilly, 'IG Reviewing Overclassification at DoD,' *Defense News*, 8 February 2012.

294 Frederick Bartell et al., Collaborating with the Private Sector, (Washington, DC: Global Innovation and Strategy Center, 2009), http://lsgs.georgetown.edu/programs/CyberProject/STRATCOM%20Report.pdf.

295 Elizabeth Goitein and David M. Shapiro, Reducing Overclassification Through Accountability, (New York: Brennan Center for Justice, 2011), http://brennan.3cdn.net/3cb5dc88d210b8558b_38m6b0ag0.pdf.

296 In Germany, some police services (illegally) engaged in CNE activity with the help of the so-called 'Bundestrojaner' ('Federal Trojan') (see Kai Biermann, 'CCC enttarnt Bundestrojaner,' *Die Zeit*, 8 October 2011.).

especially if it is potentially incriminating for the party sharing the information. LE and IC have a very different approach to the issue of self-incrimination. While the IC could very simply ignore minor illegal acts, most liberal democratic countries' law enforcement agencies have absolutely no choice in the matter: they have to investigate breaches of the law. For this reason, most information exchanges related to cyber security tend to have a stronger connection to the IC, rather than to the police itself.

## 3.4. STRATEGY DEVELOPMENT PROCESSES

The development of a NCSS, and meeting specific 'goals', requires appropriate 'means'. These means include budgets and programmed resources but fundamentally are mostly about processes. At a macro-level, most of these processes will be pre-determined by the local conditions and respective political system: should the strategy be developed from the working-level? Or should politics take the lead? There are no right or wrong answers – each variant has strong and weak points.

### 3.4.1. Bottom-Up, Top-Down and Re-Iterative

Unlike nearly all other national security issues, cyber security touches directly on nearly every citizen in a country, leading to important decisions regarding how much to involve citizens when developing policies. Citizens that are happy to allow their government to decide how to combat terrorists or negotiate with neighbours can be easily enraged if they feel their own personal computer, their personal information, or access to favourite social media sites is put at risk without their consent.

Accordingly, there is a fine balance when developing NCSS. How open or closed should the process be? Nations have so far chosen one of three paths: top-down, bottom-up or a re-iterative combination of the two. The last path is usually only available when there has already been substantial prior discussion.

France and the United Kingdom can be said to have embarked on a top-down path. National telecommunication champions and other outside voices may have had some influence in the development of their NCSS (both launched in 2011). Those central governments kept very tight control over the content, message and communication. In France, a clear hierarchy of documents aligns with the sequence of events: the 're-framing' of French security needs in the first ever National Security Strategy (NSS) in the Defence White Book of 2008; the creation of a single responsible

agency, French Network and Information Security Agency[297] (ANSSI), with a clear mandate in 2009, and the publication of an 'Information Systems Security and Defence Strategy' by that organisation in 2011. A similar process is visible in the UK. The advantages are an increased focus on the document and the development of policies is far more streamlined. However, the document may not have buy-in from civil society.

Other nations have taken the opposite approach with a 'bottom-up' process, building on the evidence and advice of working groups. The German NCSS is such an example of a bottom-up process. The 2011 document itself was the last deliverable of a longer CIP process: the general National Plan for Protecting Critical Information Infrastructure (NPSI) in 2005 and the later specific protection plans for the federal government (UP-BUND) and the private sector (UP-KRITIS) in 2007.[298] Another example of this approach was the Austrian government's 'National ICT Security Strategy' of 2012, where five working groups, composed of over 20 private stakeholders and numerous government departments, delivered recommendations on specific areas that were collated in an official document.[299]

With over a decade of debate on the subject, the United States has tried both bottom-up and top-down approaches. It now can be said to have settled into a re-iterative, hybrid state of discourse. To develop the National Strategy to Secure Cyberspace,[300] the White House led a fully public bottom-up process in 2003 in town halls across the nation to hear from citizens, and targeted meetings with privacy experts, and technology and cyber security companies. This was a very in-depth and often very frustrating (and seemingly fruitless) process, although it did ensure more acceptance of the final document. When this document was felt to be no longer sufficient, the White House took the opposite top-down approach with the Comprehensive National Cybersecurity Initiative (CNCI) which was developed behind closed doors in classified sessions five years later. It was over two years before even a summary of the CNCI was declassified and released.[301] Secrecy ensured the specific proposals did not become public, though this meant important stakeholders were not consulted, leaving some citizens uneasy.

---

297 In French: *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI).

298 See, for instance, Marc Schober, 'Aktuelles zu Kritischen Infrastrukturen,' in *SECMGT-Workshop* (DB Systel GmbH: Gesellschaft für Informatik, 2011).

299 Austrian Federal Chancellery, *National ICT Security Strategy Austria*. Note that this strategy is not the Austrian National Cyber Security Strategy which, as of September 2012, was still being drafted, but which will presumably draw heavily on the aforementioned document.

300 White House, *The National Strategy to Secure Cyberspace*.

301 White House, *The Comprehensive National Cybersecurity Initiative (as codified in NSPD-54/HSPD-23)*.

The most recent high level strategy document, the Cyberspace Policy Review of 2009,[302] was a combination of top-down and bottom-up approach that is described here as 're-iterative'. The White House Cybersecurity Coordinator led an open discussion, inviting comments to shape the document but also was in the position to reflect back on a long range of previous documents, going back over 10 years. The document repeatedly referenced the need to have clear performance metrics for cyber security – a result of which was a more standardised collection of FISMA data via a specific tool.[303] However, the process was clearly not as publicly-orientated as the 2003 effort. The final document was influenced by the non-governmental input but was undoubtedly the product of the White House staff.

## 3.4.2. Governmental vs. Societal Approaches

Cyber security policy development is not usually only an issue for government. In a number of countries, non-state actors have played an important role in helping to define their countries' NCS posture. NCS is unlike most other national security issues in that non-state actors can be said to play a crucial role. A 'societal' approach to developing a national cyber policy can be said to go beyond the involvement of certain crucial private sector companies (such as telecommunication operators or defence contractors) and include other non-state actors.

**Germany and the 'Grey Hats':** on the face of it, Germany's cyber security frameworks do not seem to imply a strong societal approach to national cyber policy. While the government master plan for improving NCS and Critical Information Infrastructure Protection (CIIP), called UP-KRITIS,[304] often makes reference to the non-state sector, the official connections between state and non-state actors are not as extensive as in other countries. The German National Cyber Security Council (NCSR[305]*)* represented one of the main innovations of the German NCSS,[306] published in 2011. This Council, which met three times 2011-2012, is more of a Whole of Government coordination group, especially suited to communicate between the Federal (Bund)

---

302 White House, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*. Note that the White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* is considered here to be a subsidiary document.

303 The Federal Information Security Management Act (FISMA) of 2002 regulates government information security practices. Although wide-scale reporting of specific metrics was always intended in FISMA, it only really could have been said to have started in the fall of 2009, based on a new collection tool (see Jason Miller, 'Agencies must use Cyberscope tool for FISMA reports,' *Federal News Radio*, 15 September 2011.).

304 German Federal Ministry of the Interior, *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen* (Berlin: German Federal Ministry of the Interior, 2007).

305 In German: *Nationaler Cyber-Sicherheitsrat*.

306 German Federal Ministry of the Interior, *Cyber Security Strategy for Germany*.

and State (Länder) level. While in all the three meetings there were representatives of the industry, they are officially only present 'upon invitation' and do not represent a standing element of the structure. Therefore, officially at least, the German version of the Council is primarily governmental[307] – even if, unofficially, the non-state sector plays a strong role. The strength of the German non-state sector can partly be seen in one example: the Chaos Computer Club (CCC). The CCC is one of the oldest (founded in 1981) and largest hacker organisations in the world and, despite having been often implicated in illegal activity, plays an important role in German civil society. They also regularly function as whistle blowers. Here, activities of the CCC include, for instance, discovering and reverse-engineering a piece of government malware,[308] the use and functions of which were explicitly curtailed by the German Constitutional Court but nonetheless employed illegally by a number of police services. The CCC is also one of the most important cyber advocacy groups advising the German legislature: few bills related to the topic are considered without CCC being involved at some stage, for instance, when the new citizen engagement Web consultation service of the Bundestag threatened to be cancelled due to cost overruns, CCC even offered to build a new one from scratch for free.[309] In German NCS, the role of the 'grey hat hackers' in CCC may be indirect, but it is certainly measurable, and very likely a unique state of affairs among liberal democracies.

**The Netherlands and the 'Cyber Polder Model':** the Netherlands has always claimed a certain spirit of public-private partnerships and consensus decision-making, a type of social-partnership known as the 'Polder Model'. It is, therefore, unsurprising that the Netherlands' NCSS puts much emphasis on a societal approach, looking in particular to involve non-state parties in cyber security decision-making. One example of this inclusive form of working is the Dutch National Cyber Security Council (NCSC), a top-level advisory body. Not only is one of the co-chairs a member of the private sector,[310] but fully eight of the 14 members of the Council can be described as non-state.[311] Even for an advisory body (in contrast, the German NCSR

---

307 Although the official description of the Council makes it clear that the private sector representatives are not full members of the Council, there are other explanations to be considered besides the apparent focus on Whole of *Government* rather than Whole of *Nation*. As other countries in Europe have already discovered, there can be major legal issues in determining which non-state actors (especially private companies) can be part of such consultative bodies and which cannot. There is a clear 'unfair competition' issue to be considered. It is, therefore, easiest to simply say that the private sector is only there upon 'invitation', and so avoid legal challenges.

308 See, for instance, Chaos Computer Club, 'Chaos Computer Club analyzes government malware,' CCC, http://ccc.de/en/updates/2011/staatstrojaner.

309 Chaos Computer Club, 'Chaos Computer Club leistet digitale Entwicklungshilfe für die Enquête-Kommission,' CCC, http://www.ccc.de/de/updates/2011/adhocracy-enquete.

310 In June 2012 this was the CEO of KPN – the largest telecom company.

311 Don Eijndhoven, 'Dutch Cyber Security Council Now Operational,' *Infosec Island*, 5 July 2011.

can be described as a supervisory body), this is a very high proportion of non-state actors and clearly represents a 'societal' approach. The Netherlands also has a further innovation in developing a Whole of Nation or societal approach. The Netherlands Organisation for Applied Scientific Research (TNO)[312] is neither state nor private, but enjoys a special constitutional status. As neither a government department nor a company, the TNO was well placed to run the main public-private partnership for a cyber security information exchange hub: the Centre for the Protection of National Infrastructure (CPNI.NL).[313] The immediate predecessor of the CPNI.NL, known as National Infrastructure against Cybercrime (NICC), had owed part of its success to the impartiality with which it was able to treat the security services (e.g., the ability to enforce a 'share or quit' rule within the individual information exchanges). It is perhaps doubtful that a government ministry would be similarly impartial.

### 3.4.3. Resources, Budgets and Metrics

In essence, all NCSS-type documents are first and foremost a guideline on how resources will be allocated in the future. Similar to a NSS, it is not necessary or common practice for a specific allocation of resources to be made within the document itself. Many NSS documents are, in fact, produced before such budgets have been set, in part to set the framework for the necessary discussions. What does have to be understood is that a strategy without assigned resources, in particular, a budget, is only of marginal value. It is of secondary importance if this budget is simply reprogrammed from existing budgets, or indeed constitutes new funds – what is important is that funding is available to carry out the intended activities.

Very few nations publicly disclose their relevant NCSS budgets and, if they do so, they are largely classified in detail. The UK was one such example. Despite assigning £650 million to the National Cyber Security Programme in the Cyber Security Strategy, the vast majority of this funding[314] went directly to the single intelligence account in the budget. However, despite the lack of clarity as to where exactly the additional funding was going (or, indeed, how 'additional' it actually was), the number of '£650 million for UK cyber' made for an excellent strategic communication device and was widely quoted in the media.

The question of how to measure performance in cyber security is still largely inconclusive. Most attempts have involved varying attempts at providing a Return

---

312 In Dutch: *Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek*.

313 At time of writing it was, however, unclear if the CPNI.NL will remain at the TNO.

314 Dave Clemente, Defence and Cyber-security, (London: UK Parliament, 2012), http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs02.htm.

on Investment (RoI) framework to security, a process that often fails based on the difficulty of quantifying the gains with any reliability.[315] The collection of any metrics to measure any cyber security performance can be a considerable challenge. The United States, with a strong tradition in performance management indicators, produces a number of metrics at various levels.[316]

## 3.5. ENGAGEMENT WITH STAKEHOLDERS

Fundamentally, any approach to NCS will have three different sets of stakeholders: governmental, national (societal) and international. As was explained in Section 1, the approach used here to model the engagement of these stakeholders derives from terms that originated within public policy theory at large, and which focus on how policy is delivered: via Whole of Government (WoG), Whole of Systems (WoS), and, more recently, Whole of Nation approaches (WoN).[317] Overall, they focus on the principal security challenge of the 21st century: the need for a wide range of different actors to work together on a very wide range of security-related themes. These concepts first entered security policy language within the context of peace building in conflict zones such as Afghanistan and Iraq, and are closely identified with related concepts within international security, such as 'Fragile States' and 'Conflict Prevention' policies.[318] Increasingly, these approaches are being applied

---

315 One such attempt of quantifying these gains is ROSI, or Return on Security Investment. There are a number of different methods on how to exactly accomplish this but, for an example of integrating ROSI with the COBIT risk management system, see ISACA, G41 Return on Security Investment (ROSI), (Rolling Meadows, IL: ISACA, 2010), http://www.isaca.org/Knowledge-Center/Standards/Documents/G41-ROSI-5Feb10.pdf.

316 Examples of these metrics include the three high-level CAP metrics for measuring cyber security (see US Government, 'Using Goals to Improve Performance and Accountability,' Performance.gov, http://goals.performance.gov/goals_2013.), and the monthly reporting practice in-line with the FISMA legislation using the 'cyberscope' tool (see Greg Schaffer, *Federal Information Security Memorandum. FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, ed. US Department of Homeland Security (Arlington, VA 2012).)

317 For an example of how the Department of Homeland Security is using the 'Whole-of-X' terminology for cyber security see Janet Napolitano, State of America's Homeland Security Address [Remarks], (Washington, DC: Department of Homeland Security, 27 January 2011), http://www.dhs.gov/news/2011/01/27/state-americas-homeland-security-address.

318 The WoG approach has been developed particularly in the context of the OECD Development Assistance Committee's (DAC) Fragile States Group (FSG). See OECD, Whole of Government Approaches to Fragile States, (Paris: OECD, 2006), http://www.oecd.org/dac/conflictandfragility/whole-of-governmentapproachestofragilestates.htm. For an overview of these and related concepts see Kristiina Rintakoski and Mikko Autti, Comprehensive Approach. Trends, Challenges and Possibilities for Cooperation in Crisis Prevention and Management, (Helsinki: Finish Ministry of Defence, 2008), http://www.defmin.fi/files/1316/Comprehensive_Approach_-_Trends_Challenges_and_Possibilities_for_Cooperation_in_Crisis_Prevention_and_Management.pdf. For WoN interpretations see, for instance, Michael G. Mullen, 'Working Together: Modern Challenges Need 'Whole-of-Nation' Effort,' *JFQ* 4, no. 59 (2010).

to NCS, as they address the most basic issue of NCS: the reality of the increasing 'diffusion of power'[319] among various actors, most of them non-state.

### 3.5.1. Whole of Government (WoG)

Originally, the Whole of Government approach (WoG, known in the UK as 'joined-up government'[320] and also known as 'networked government') was conceived primarily as a cost-saving measure: government departments were encouraged to pool resources and to deliver 'more for same.' At the same time, many policy-makers were starting to identify the comprehensive international failure in the Balkans in the early 1990s with a complete lack of coordination among all actors. Consequently, WoG concepts were developed. The most prevalent of such concepts today is the so-called '3D Approach' (for Diplomacy, Development and Defence),[321] first applied by Canadian forces in Afghanistan in 2004 and used today by many Western governments, including the United States.[322]

Applying this approach to NCS is increasingly viewed as being key to success in national cyber security. As was remarked upon in Section 1.4, the challenges for NCS extend over a wide number of different specific fields, or mandates. These mandates can, for instance, range from military cyber operations to diplomacy and counter cyber crime. Each of these mandates is infused with its own strategic goals, language and basic philosophy. The fundamental differences mean that, even two seemingly closely related approaches such as the IC and LE can approach a subject such as cyber crime from very different angles.

In practice, this means that the esoteric nature of the individual mandates naturally leads to 'stovepiping' in narrowly defined government organisations. In the worst case, this means that a number of different organisations and governmental departments will work on a similar subject (e.g., cyber crime legislation) and not coordinate with each other. This failure at a policy level can also easily be duplicated by a failure at the practical, operational level. In countries that are just in the process of formulating a NCSS it is quite normal to see a highly fragmented cyber defence landscape: each ministry or department will often be responsible for their

---

319 Nye, *The Future of Power*.

320 For an Australian example see State Government Victoria, Victorian approaches to joined up government. An overview, (Melbourne: State Services Authority, 2007), http://www.ssa.vic.gov.au/images/stories/product_files/71_joined_up_government.pdf.

321 See Robbert Gabriëlse, 'A 3D Approach to Security and Development,' *PfP Consortium Quarterly Journal* 6, no. 2 (2007).

322 Critics have often remarked that, going by budget allocations, it should really be 'Defence, Diplomacy and Development', as the money spent on 'Defence' in Afghanistan is more than a factor higher than spent on 'Development'.

own networks. More advanced cyber nations are aware that this highly fragmented approach is a losing proposition in the longer term,[323] and seek to empower at least a central coordinating body within the operational (and often policy) levels of government.

Building coordination among government departments is probably one of the most important tasks of any grand strategy within NCS. The US DoD, for instance, clearly stated in its 2011 'Strategy for Operating in Cyberspace' that one of its five main initiatives was 'to enable a whole-of-government cybersecurity strategy.'[324] Similar goals have been expressed in India,[325] New Zealand,[326] Canada,[327] Australia,[328] Germany[329] and other countries. Increasingly, however, countries go beyond the emphasis of WoG and are seeking to emphasise the societal or national view: the Whole of Nation approach.

### 3.5.2. Whole of Nation (WoN)

For NCS, the importance of the private sector and the civil society is obvious. The private sector is responsible for virtually all of the software, hardware, and services which are exploited for cyber attacks, maintains most of the network infrastructure over which these attacks are conducted, and often owns the critical infrastructure that these attacks are directed against. Furthermore, civil society actors, as distinct from the private sector, dominate cyberspace. Civil society actors define the programmed parameters (e.g., the software protocols) of the cyber domain, as well as executing, researching and, ultimately, publicly speculating on cyber attacks. Together, these non-governmental actors account for the bulk of what is termed 'national' cyber security.

---

323 There is an argument that a highly fragmented governmental cyber defence (e.g., each ministry having its own CERT) provides for some 'resilience', or defence in depth, through diversity. While this is also true, this approach to resilience is enormously expensive and, ultimately, will still have all the disadvantages of the small organisation while it is unlikely to implement all the more significant needs a true resilience strategy would entail.

324 US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*: 8.

325 Press Trust of India, 'PM-led National Security Council discusses cyber security,' *Daily News and Analysis*, 28 June 2012.

326 The term 'all of government' is used in New Zealand (see New Zealand Ministry of Economic Development, *New Zealand's Cyber Security Strategy*.).

327 Canadian Security Intelligence Review Committee, Checks and Balances. Viewing Security Intelligence Through the Lens of Accountability, (Ottawa: Canadian Security Intelligence Review Committee, 2011), http://www.sirc-csars.gc.ca/pdfs/ar_2010-2011-eng.pdf. 18.

328 Australian Government, 'Cyber Security Policy and Coordination Branch,' http://www.ag.gov.au/Organisationalstructure/Pages/CyberSecurityPolicyandCoordinationBranch.aspx.

329 German Federal Ministry of the Interior, *Cyber Security Strategy for Germany*.

It was the realisation of the importance of non-state actors which provided the impetus for developing the Whole of Nation approach (WoN), both in cyber security specifically, but also in a number of different security policy fields. WoN, as opposed to WoG, goes under many different names but the intent is usually the same: improved cooperation between national state and non-state actors, the latter including utilities, academia, ICT companies and even private individuals. Exactly how the 'increased cooperation' is achieved is, of course, subject to different national political systems and cooperations. Countries with stronger central government seem to view WoN as a legal instrument to enforce compliance from non-state actors in situations of national danger. This is not dissimilar to the approach of total defence popular among smaller European countries in the Cold War. The majority view in liberal democracies is to treat the federal government as the 'primus inter pares' among a number of different stakeholders; stakeholders that often need to be convinced, rather than forced, to cooperate. However, there remains little thinking in many countries as to how the military would protect critical infrastructure under determined assault by another nation. Often, the defence ministry is concerned with the resilience of the private sector only as far as it ensures continuity of its own operations.

The first example of WoN is often within the critical infrastructure protection mandate. This encompasses infrastructure that is often overwhelmingly held in private hands and NCS has a direct national interest in helping protect these companies from cyber attack. The cooperation between the state and non-state sector at the very least includes agreeing on basic risk management standards, but usually goes much further. Other components include common risk analysis frameworks, operational information exchange, and even common operational cyber defence structures.[330] CIP is, however, not the only focus of a WoN approach in the cyber domain. Depending on the focus, this approach can come to include diverging concepts such as child safety online and paramilitary 'cyber militias.'[331] Overall, it is possible to differentiate three different levels of cooperation: the defence, security and critical infrastructure level; the commercial cyber security level, and the civil society level. Each level is critical – the civil society level, for instance, is responsible for not only aspects such as data protection and internet freedoms but is, technically speaking, the driving force behind the World Wide

330 The possible deployment of the US federal EINSTEIN 3 Intrusion Prevention System to members of the national critical infrastructure programme is one, hotly debated, example. For an analysis of that debate see Steven M. Bellovin et al., 'Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure,' *Harvard National Security Journal* 3, no. 1 (2011).

331 An example of this is the Estonian Cyber Defence League. See, for instance, Luukas Ilves, 'Cyber Security Trends and Challenges,' in *Cyber Security Trends and Challenges: Latvian and Estonian Perspective* (Riga: CERT.LV, 2012).

Web (see Section 3.3.3). This diversity illustrates that WoN is primarily a catch-all term, intended to encapsulate all non-state activity relevant to national security.[332]

Within a few years the term 'Whole of Nation' has gone from complete obscurity to recognised lingo within the National Security Council[333] and other parts of the US government – equally, the term 'Whole of Society'[334] is often employed. The term has also been used in Australia for a number of years in security policy documents.[335] The definition of the term 'Whole of Nation' varies according to its contexts – indeed, there are no accepted universal definitions. In the UK, the WoN approach is equivalent to the 'Comprehensive Approach', which has also been applied to cyber,[336] besides numerous other security topics. In the Dutch National Cyber Security Strategy, the term 'network-centred form of collaboration'[337] is used to discuss the same process. In Germany, the term '*gesamtstaatlich*' is a close equivalent, and often used in the NCS related discourse,[338] although the German military also talks about using networked security (*Vernetzte Sicherheit*) as a type of comprehensive approach. In most cases, the WoN approach is an attempt to facilitate cooperation. When applied to the private sector, it represents the essence of the 'self regulation where possible, legislation where necessary' approach.[339] Consequently, the most important WoN organisations are wide-reaching advisory bodies with strong non-state contributions (e.g., the Dutch Cyber Security Council).

---

332 In France, there have been a number of documents which illustrate the importance of the private sector in general and the critical infrastructure (*infrastructure vital*) in particular. See, for instance, Roger Romani, *Rapport d'informations sur la cyberdéfense* (Paris: Sénat, 2008). 48-50.

333 See Homeland Security News Wire, 'GAO: U.S. slow to implement president's cyber security strategy,' *Homeland Security News Wire*, 20 October 2010.

334 See, for instance, Mike Anderson, 'Trojans, Malware and Botnets got you down...?,' *United States European Command*, 24 January 2012.

335 One of the first mentions of WoN occurred in Australia in 1997.See Australian Department of Foreign Affairs and Trade, *In the National Interest. Australia's Foreign and Trade Policy White Paper* (Canberra: Australian Department of Foreign Affairs and Trade, 1997). For a more recent analysis see Anthony M. Forestier, 'Effects-Based Operations: An Underpinning Philosophy for Australia's External Security?,' *Security Challenges* 2, no. 1 (2006).

336 See UK Home Office, *Cyber Crime Strategy*. Also see UK Cabinet Office, The National Security Strategy of the United Kingdom: Update 2009. Security for the Next Generation, (Norwich: The Stationery Office, 2009), http://www.official-documents.gov.uk/document/cm75/7590/7590.pdf.

337 Dutch Ministry of Security and Justice, 'The National Cyber Security Strategy. Strength Through Cooperation,' (The Hague: Dutch Ministry of Security and Justice, 2011), 9.

338 German Federal Ministry of the Interior, *Cyber-Sicherheitsstrategie für Deutschland* (Berlin: German Federal Ministry of the Interior, 2011). 5 and 12.

339 As in Dutch Ministry of Security and Justice, 'The National Cyber Security Strategy. Strength Through Cooperation.'

### 3.5.3. Whole of System (WoS)

With the growth in popularity of the '3D Approach' in so-called Stabilisation Operations, such as Afghanistan, there came increased criticism, in particular by development and aid organisations. As independent, non-state actors working internationally, they certainly did not see themselves as being subject to any type of WoG effort to 'coordinate' them. Their world was flat hierarchy, international and made up of very similar organisations with shared values and organisations (e.g., an interconnected 'system'). To illustrate their independence, these organisations started using the Whole of System approach (WoS) to talk about increased cooperation among what has become known as 'like-minded actors'.[340] It was not only civilian aid groups that liked the implication that they were organisations independent from government coordination, but both NATO and the European Union also developed their own concepts of WoS which illustrated their international mandates.[341]

In cyber security as well as in 'Fragile States' policy, international cooperation does not only mean 'between governments'. Cyber security is overwhelmingly an issue addressed by non-state organisations. For instance, the international Forum of Incident Response and Security Teams (FIRST) group of accredited CERTs play a major role in facilitating international cyber security (also for governments), but is itself rooted within academia. Within the field of internet governance, the 'technical' component is often addressed via organisations such as the IETF and IEEE.[342] Being composed largely of volunteers and (increasingly) private sector representatives, the role of government here is rather limited. Government, especially if it is committed to 'multi-stakeholder governance',[343] cannot claim much direct influence on these groups' work. It can encourage them to self-organise and generally seek to provide an open door to possible engagement. Governments have a stronger input with policy-focused organisations, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the ITU, but especially within issues of 'cyber

---

340 The 3D of the WoS approach has been called '3C' (for Coherent, Coordinated and Complimentary) and was particularly developed by the OECD-Development Assistance Committee. See, for instance, OECD, A Comprehensive Response to Conflict and Fragility, (Paris: OECD, 2009), http://www.oecd.org/development/conflictandfragility/44392383.pdf.

341 The EU WoS approach is often called the Whole of the Union approach. While often used as a shorthand for simple agreed-upon action among members, often the term is used to imply the need for directly assigned organisational assets (such as helicopters or the like). The NATO WoS approach is more operational and was encapsulated as the 'Comprehensive Approach'. The most recent addition to this thinking is the term 'smart defence', which seeks to look at a better pooling and sharing of resources.

342 The Internet Engineering Task Force, and Institute of Electrical and Electronics Engineers, respectively.

343 As defined in Council of Europe, *Declaration by the Committee of Ministers on Internet governance principles* (Strasbourg: Council of Europe, 2011).

diplomacy.'[344] This rapidly evolving field deals with issues such as norms of state behaviour in cyberspace, and discussing confidence building measures between states.

**Table 6:** Differences Between WoG, WoN and WoS

| | Whole of Government | Whole of Nation | Whole of System |
|---|---|---|---|
| Synonyms | Joined-Up Government, Networked Government | Whole of Society Approach | Whole of the Union, Whole of Alliance/Coalition |
| Related Concepts | 3D Approach (Diplomacy, Development, and Defence) | Comprehensive Approach | 3C Approach (Coherent, Coordinated and Complementary) |
| Actors Involved | - Central Government<br>- State Government<br>- Local Government | - Contractors/CIP<br>- ICT/Security Specialists<br>- Civil Society/Academia | - Diplomats<br>- Internet Governance Stakeholders<br>- Industry/Scientific/ Technical Working Groups |
| Main Working Mode | Coordination | Cooperation | Collaboration |
| Cyber Security Examples | OCSIA (UK) | CSC (NL) | ICANN |

This complicated international dimension of cyber security has not always been fully understood. While most early NCS documents pay lip service to the transnational nature of cyber, the realisation that it is needed to play a key role in such strategies only developed in recent years. A consistent challenge was that, despite having the word 'international', the WoS approach to cyber security usually goes beyond the activities of the relevant foreign ministries. When the US drafted the 'International Strategy for Cyberspace' in 2010-11, 18 different government agencies contributed to the vision.[345] As the US experience showed, the bundling of very different views from different mandates is a complicated, arduous process but it needs to be done.

---

344 As defined in Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, 7. However, Potter was referring to 'e-diplomacy' which is interpreted here as the ability to enable diplomacy with new media.

345 See Colleen O'Hara, 'Global Cyber Sleuth. The State Department's Chris Painter relishes his role as a cyber diplomat,' *Leadership* Winter (2012): 43.

In NCSS created during and after 2010, 'international cooperation' is always ranked as one of the top five initiatives.[346]

### 3.5.4. National Cyber Security: Coordinate, Cooperate and Collaborate

Each of the 'dimensions' described above refers only to one particular aspect of NCS: the importance of working with other actors within different contexts. This probably remains one of the single most important success factors in NCS. In this context, one can distinguish between three main working modes:

**Coordination**: within government, the challenge is to develop a unity of purpose across the different levels and types of government – especially within federal government and between federal and local structures. Although national political systems differ greatly, the intended effect will always be the same: the improved coordination of national efforts. As the term 'coordination' implies, this is only possible where there is a clear legal mandate to exercise control over functions situated in different parts of government. This can be a considerable challenge. In many liberal democratic governments, even the head of the government function (e.g., a prime minister's office or similar) does not have the authority to order other parts of the national government. Even more difficult is the situation in political systems that are heavily federalised. In these systems, state and local governments (which of course can include major cities and national critical infrastructure) are often totally independent from central government on cyber security issues. Although most political systems have measures in place to ensure central control in case of a significant national emergency, the very information security measures that are supposed to prevent such emergencies are often not coordinated, greatly raising the risk of a significant cyber security event occurring.[347] Addressing the coordination issue that exists both between, as well as within, the individual levels of government (central, state and local) nearly always represents one of the most significant challenges for NCS.

**Cooperation:** a further significant challenge for government represents non-state actors, both organised and non-organised which, as has repeatedly been pointed out, are absolutely central to all types of NCS issues. Within the larger, societal

---

346 This includes the French Cyber Defence Strategy, as well as the UK, Dutch, German and other strategies published within that time frame.

347 There is an opinion that 'overcentralise' is actually the worse thing for NCS. This view states that diversity in both information security standards and especially ICT hard- and software represents the best assurance against a major cyber attack. Even within the most extreme interpretation of this view it is necessary, however, to have a single body that at least can ensure that certain activities are not duplicated, especially when these activities would certainly interfere with each other.

aspect (WoN) the legal powers of the government will often be less clear and, in essence, secondary. This becomes obvious when the entire scope of necessary action across all national or societal components is examined. Certain non-state enterprises (such as defence contractors and perhaps even all critical infrastructures providers) may be directly regulated by the state. In some cases there might even be classified communication channels and exchanges of information. But there are limits to how far this could go. On a second level of analysis, for instance, other companies (such as virtually all the software companies as well as the hardware and ICT security companies) will not be addressed by any CIP legislation. The contribution of these companies, even when they are not directly connected to a national security infrastructure, is immense and often crucial. But they will seldom be the target of specific regulations and thus cannot be 'ordered' to do anything by the government. Even more difficult is the situation when a third and final analysis is applied: the smaller non-organised non-state actors. This includes small civil society, advocacy and research groups, and even includes individual bloggers and key technical volunteers. This group represents a major force in internet governance (indeed, it can be claimed that the internet is largely built by such individuals) but, due to their small individual size or non-hierarchal organisation, are very difficult for government to engage with. Legislative measures, at least within liberal democracies, can, therefore, never be comprehensive enough to be able to coordinate the non-state sector. The government instead can only encourage the voluntary cooperation among these actors, and this usually, in turn, depends on transparency and trust in relationships that can only be built over time.

**Collaboration:** within the international dimension (WoS) the elements of governmental collaboration and the national/societal cooperation becomes most apparent. From a government point of view this dimension can be roughly segmented into three layers and these illustrate the importance of the non-state actors in the domain. At the first, diplomatic, level, government reigns supreme, but even here non-state actors often play a crucial role – in particular within Track 1.5 bilateral discussions[348] and similar. At the second level, which includes internet governance and related activities, government already often has a minor role, especially within technical matters. Finally, at the third level, there are a galaxy of related scientific and industry working groups as well as other organisations. The government plays a very minor role. In fact, many of the technical standards and industry collaborations are agreed upon without any government influence whatsoever. The government will never be able to legislate itself through this environment – not only will other nations not necessarily want to adopt an alien agenda but the non-state actors of a particular nation will probably not just mutely

348 This refers to 'unofficially official' diplomatic exchanges, mostly conducted with the help of non-state actors. See Sections 2.3.3 and 4.5.1.

submit to a government agenda when it clashes with their own. Indeed, the opposite requirement is the case: government often does not understand international cyber security requirements, and completely depends on the non-state sector to help inform Track 1 (official) diplomatic discussions. In the contexts of international cyber security discussions, governments must appreciate this when dealing with foreign governments, giant transnational corporations, and little anarchic groups of programmers.

## 3.6. STRATEGIC PITFALLS, FRICTIONS AND LESSONS IDENTIFIED

When creating a NCSS, there are a number of lessons that can be taken from other policy development processes, for instance, from developing conflict prevention frameworks and similar. These have been dealt with elsewhere.[349] Here, a couple of macro trends are listed instead:

**Underestimating Talk:** as has been indicated above (Section 3.5.4), the need to work within an environment defined by the increased 'diffusion of power'[350] is perhaps the greatest challenge to government. The plethora of actors that need to be engaged to exercise NCS represents not only a conceptual challenge to government (adjusting to unclear hierarchies, unofficial mandates, and uncertain legal basis), but a considerable resource challenge as well. The necessity of engaging with all these actors is often much more time consuming than, for instance, policy development. But it is this engagement that builds trust, and basic trust is more important than any policy document.

**Overestimating definitions:** clarity of communication and concepts is extremely important. However, specific definitions are one of the most elusive components of cyber security. Between individual government mandates, let alone nations or ICT security interest groups, there is often a wide variety of specific definitions or legal frameworks that are used. This is partially due to the nature of the evolving cyber domain and, when evaluating strategy and strategic frameworks, it is necessary to be aware of fundamentals and not let oneself be constrained by the particular language of the forum in which one is operating. For this reason, any adjustment to legal frameworks has to pay particular attention to the vagaries and implications of

---

349 See Alexander Klimburg, 'Lessons from the Comprehensive Approach for Whole of Nation Cybersecurity,' *Per Concordiam* 2, no. 2 (2011). (For a German version of this article see Alexander Klimburg, 'Gesamtstaatliche Ansätze zur Cybersicherheit. Erfahrungen aus Österreich,' in *Strategie und Sicherheit 2012. Der Gestaltungsspielraum der österreichischen Sicherheitspolitik*, ed. Johann Pucher and Johann Frank (Wien et al.: Böhlau Verlag, 2012).)

350 See Nye, *The Future of Power*: 113-51.

specific definitions – not because these legal frameworks will determine the course of cyber security in the future, but because those frameworks will be ignored if the definitions they use do not reflect the true fundamental needs of NCS. It is often much easier and more useful for policy-makers to develop useful descriptions outlining general concepts, rather than fixating on tight definitions.

**Encouraging path dependency:** a major challenge to cyber security is the esoteric nature of the subject. Few issues relevant to national security are as multi-faceted and complex, or more dependent on confidential or secret information as sources of knowledge. This has encouraged a number of bottom-up processes. Essentially, these are viewed as positive developments, as they often are built on a sound technical basis. Unfortunately, in some cases, this can lead to essential strategic decisions being taken within a very narrow (and low level) strategic framework. Many organisations will strive to accomplish their specifically assigned goals (be it in intelligence collection or cyber defence, or similar) and will thus give themselves the greatest amount of leeway and resources to accomplish their mission. Changes to facilitate a particular task at this level can, however, greatly impact the core values of a nation. This can occur without the strategic or political level being fully cognisant of what is occurring – be it towards data protection, due process in awarding commercial contracts, investment in key infrastructures and technology, the use of law enforcement means, or the launch of offensive cyber attacks. At the strategic level, care must be paid to overtly delegating responsibility for these issues. The results could be quite the opposite of what policy-makers were aiming for.

**Ignoring Flexibility:** 'learning by doing' is a core element of most policy development processes, and, in NCS, it is absolutely vital. Rapid technological change and a variety of unknown unknowns (e.g., the true extent of the interdependence of critical infrastructures) mean that most policy documents, regulations, and even political and legal frameworks, are unlikely to withstand their first trial by fire without major challenges. In-depth operational exercises, exchange of lessons learned, and an emphasis on continuous policy development can help, but do not replace the basic need to continuously question basic assumptions. Otherwise, a lack of flexibility could easily spell disaster.

## Office of Cyber Security and Information Assurance (OCSIA)

The Office of Cyber Security and Information Assurance (OCSIA) of the United Kingdom is a strategic coordination body that is a good example of the Whole of Government approach (WoG). Originally formed in 2009, it became the Office of Cyber Security and Information Assurance (OCSIA) in 2010. The OCSIA coordinates nearly all cyber security programmes run by the UK government that are directly relevant to national cyber security. Most importantly, it is responsible for the allocation of the (£650 million strong) National Cyber Security Programme funding. It has four main priorities: improving national cyber security, improving cyber defence of critical infrastructure; combating cyber crime and enhancing education and skills.

As part of the UK Cabinet Office, OCSIA provides strategic direction to all UK government stakeholders for cyber security and information security and is responsible for keeping the Cabinet and the National Security Council apprised of developments in this area. OCSIA is not an intelligence organisation but works closely (and is partially co-located with) the Cyber Security Operations Centre (CSOC), based within the headquarters of GCHQ.

## Internet Corporation for Assigned Names and Numbers (ICANN)

The Internet Corporation for Assigned Names and Numbers (ICANN) is a strategic coordination body that perhaps best represents the Whole of System approach (WoS). As a private, non-profit corporation headquartered in California, ICANN is a global multi-stakeholder organisation, meaning that while governments have a voice, so do the private sector, technical experts, and civil society. Almost anyone can join ICANN working groups in a bottom-up, consensus-driven process. ICANN is, in effect, granted its mandate through a contract with the US Department of Commerce and the US government does have a special role to play. Nonetheless, ICANN is not subordinate to any government.

ICANN is responsible for the operation and coordination of many of the critical, behind-the-scenes functions that keeps the internet functioning. In particular, it helps maintain and secure the Domain Name System, the 'telephone book' of the internet that makes it possible to use names instead of internet Protocol (IP) numbers to navigate. As ICANN takes a tiny portion of sales for certain top-level domains (such as .com) it has grown in-line with the internet and, in 2011, had a budget of over $60 million.

## The Dutch Cyber Security Council

The Dutch Cyber Security Council (CSR) was officially set up on the 30th of June 2011 by the Dutch Minister of Security and Justice on the basis of the Dutch National Cyber Security Strategy. The CSR is responsible for proactively and reactively advising the government and the private sector of cyber security and threat developments: advising on R&D, education and awareness issues, and reviewing the state of cyber security legislation from the point of view of human rights and data protection. Although officially in an advisory and not a supervision role, the Council is made up of high-ranking members from the private and public sector who have the ability to request restricted information to help formulate their own opinion. The CSR has released some of their comments and criticisms to the public.

The CSR is staffed with resources from the public and private sectors as well as from the R&D and academic communities. The Council is publicly-privately co-chaired by the National Coordinator for Counter-terrorism and Security, and the CEO of KPN Telecom. The Council meets at regular intervals but also had several meetings during the DigiNotar cyber security incident. In a national crisis situation, the CSR forms its own Whole of Nation crisis management 'ICT Response Board' (called IRB) from technical resources in the private and public sector. The IRB can directly engage with the wider cyber security community and pass recommendations and information, via the CSR, directly to the top of the national crisis management hierarchy.

# 4. ORGANISATIONAL STRUCTURES & CONSIDERATIONS

*Eric Luiijf, Jason Healey*

**Section 4: Principal Findings**

- Essentially, national cyber security (NCS) can be split into five distinct subject areas or mandates. These 'Five Mandates' are Military Cyber, Counter Cyber Crime, Critical Infrastructure Protection (CIP) & Crisis Management, Intelligence/Counter-Intelligence, and Cyber Diplomacy & Internet Governance.
- These mandates can be mapped along all stages of a cyber incident, as well as all four levels of government: the political/policy, strategic, operational, and tactical/technical levels.
- Further, these Mandates connect with 'cross-mandates': Information Exchange & Data Protection, Coordination, as well as Research & Development and Education.
- While it is important to understand the uniqueness of each of the five mandates, it is even more important to understand their commonalities, and their need for close coordination.
- A wide range of organisations engage in international cyber security activities. The most relevant of these are often not state but non-state groups.
- A lack of understanding of the mandates can lead to stovepiped approaches resulting in conflicting legal requirements and friction between cyber security functions, organisations and capabilities.
- Assigning resources without a policy can be as dangerous as drafting a policy without assigning the resources.

## 4.1. INTRODUCTION

The purpose of this section is to review specific types of national cyber security (NCS) areas (also called 'mandates') and examine the organisational and collaborative models associated with them. Before discussing the wide variety of organisational structures at the national and international levels, a decomposition model will be presented that delineates both common and specific cyber security functions, capabilities, and responsibilities along three different axes (Section 4.2). On the one hand we will distinguish between five NCS mandates. This section expands Klimburg's[351] segmentation and supplements it by three additional cross-mandates. Other axes are the cyber security incident response cycle and the various levels of decision-making. This decomposition model shall assist the reader in understanding the rationale behind the functions, responsibilities, and capabilities of organisations involved in cyber security as entities which, over the years, have been shaped by the specific division of tasks between the government, its agencies, public organisations, associations, and private companies. Section 4.3 provides an overview of the stakeholders involved in the provision of cyber security.

Taking the decomposition model as the point of departure, Section 4.4 strives to determine the main focus of analysis along the five mandates mentioned in Section 1 and three cross-mandates. Building upon this framework, Sections 4.5, 4.6 and 4.7 introduce the common set of national and international organisations. It is important to note that these sections also pay due attention to the special tasks which may be recognised by, and assigned to, various organisational subunits or organisations all belonging to one and the same mandate, or to a single service organisation in one of the mandates with the aim of supporting the other mandates. Finally, Section 4.8 will discuss some organisational pitfalls and lessons identified when addressing cyber security at the national level.

## 4.2. DELINEATING ORGANISATIONAL FUNCTIONS, CAPABILITIES AND RESPONSIBILITIES

To position the many cyber security functions, capabilities and responsibilities at the national and international levels, an analytical framework can be useful for further discussion. While there are certainly a number of methods that can be employed, the approach applied here focuses on three closely connected building blocks: the NCS mandates and cross-mandates; a generalised tool to analyse organisational conduct at large, and the incident management cycle.

---

[351] See Klimburg in Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65)*. 15-9.

A first decomposition is to split the functions across the five perspectives (called mandates) as described at more length elsewhere[352] and in Section 1.[353] These mandates include: (1) Internet Governance and Cyber Diplomacy, (2) Cyber Crisis Management and Critical Infrastructure Protection (CIP), (3) Military Cyber Operations, (4) Intelligence/Counter-Intelligence, and (5) Counter Cyber Crime. This approach is supplemented by three additional cross-mandates that work across all the mandates equally. They include (1) Coordination, (2) Information Exchange and Data Protection, and (3) Research and Education.

### 4.2.1. Across the Levels of Government

An obvious, second way of decomposition is a vertical one, perpendicular to each of the mandates and cross-mandates. Along four distinct levels of analysis, this approach combines both a military and a political understanding of war.

The two probably most succinct (and opposing) notions on the nature of war equally address the most important relationship between the act of war and the political sphere: either '[w]ar is a mere continuation of policy',[354] or '[p]olitics is the continuation of war'.[355] It is long understood that it is necessary to combine the military and the political perspective into a more comprehensive approach of understanding conflict, such as was done in the US military construct of state-conflict.[356] By adding a 'political' or 'policy'[357] level on top of the traditional war-fighting triangle (which is composed of the strategic,[358] operational[359] and tactical[360] levels),[361] this model goes beyond a purely military understanding of military operations.

---

352 See ibid.

353 See Klimburg in Section 1.5.4.

354 Carl von Clausewitz, *On War* (London: Penguin Books, 1982 [1832]). 119.

355 Michel Foucault, *'Society must be defended': Lectures at the Collège de France, 1975-1976* (New York: Pan Books Limited, 2003). 15.

356 David W Barno, 'Challenges in Fighting a Global Insurgency,' *Parameters* 36, no. 2 (2006).

357 Defined as: 'principle or course of action' (see Policy, *Oxford English Dictionary Online* (Oxford University Press, 2012)).

358 Defined as: 'the art of projecting and directing' (see Strategy, *Oxford English Dictionary Online* (Oxford University Press, 2012)).

359 Defined as: 'a planned and coordinated activity involving a number of people' (See Operation, *Oxford English Dictionary Online* (Oxford University Press, 2012)).

360 Defined as: 'skilful in devising means to ends' (See Tactical, *Oxford English Dictionary Online* (Oxford University Press, 2012)).

361 In the civil context, the operational and tactical levels of decision-taking are often reversed. In this section, however, we will use the military naming order: strategic, operational and tactical.

To go even further, it is suggested here that the four-level construct can be applied as an instrument to study the much broader context of organisational decision-making structures in government at large. As such, the four levels can be transformed into a more generalised analytical tool including: policy level where long-term political objectives are defined (e.g., a 'White Book' announcing cyber security as a top national priority); a strategic level where organisations are set up to achieve the predefined objectives (e.g., a directive establishing a specific body to achieve cyber security); an operational level where the different tasks within an individual organisation are coordinated (e.g., the segmentation of an organisation into different departments), and a tactical level where the specific tasks are ultimately executed (e.g., the specific tactics, techniques and procedures that are employed for each task). This delineation will be used for the positioning of organisational functions and capabilities only – in particular, to help provide possible examples for operational NCS institutions. Up front, it is important to remark that a strict separation of decision-taking processes into strategic-operational-tactical institutions does not necessarily reflect the actual reach of operational or tactical institutions. Effectively, a tactical level institution (say, a Computer Emergency Response Team within a crisis management unit) can take decisions that have global consequences, impacting not only the strategic but also, potentially, the political level as well.

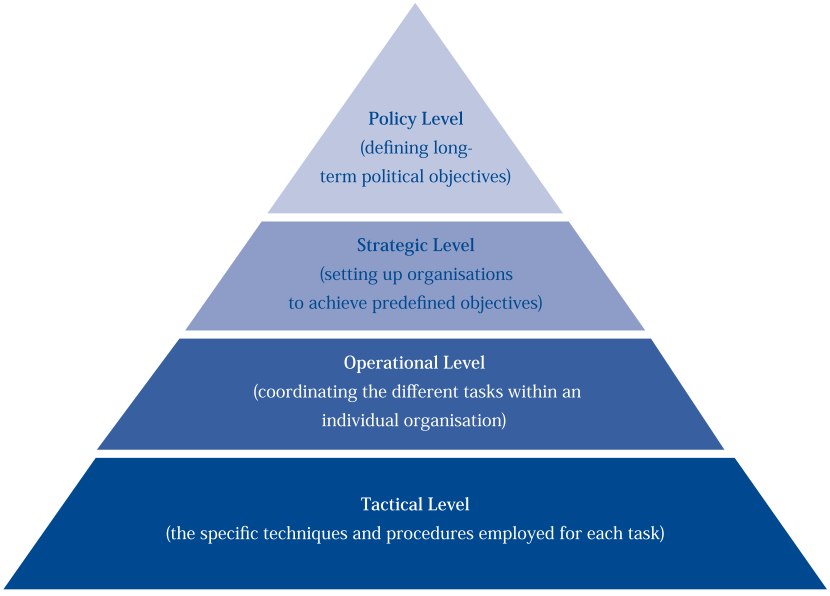


**Figure 3**: The Four Levels of War as a Generalised Tool for Analysis

It is required that the organisational responsibilities are assigned at each of these levels. In many cases, however, a clear distinction between the various levels can be difficult. Sometimes specific tasks (at the tactical level) are 'bolted on' to the organisations or to strategic goals to which they are only partially suited. Indeed, this misalignment of specific tasks to unsuited organisations, levels or even mandates is a major challenge for national cyber security. The organisational embedding of a national Computer Emergency Response Team (CERT) function[362] in a number of nations is a good example of such a misalignment. In various nations, the government CERT function has been a quick fix add-on to an existing government organisational structure. Often, this crucial tactical function is not tied into the most appropriate vertical decision-making structure or, indeed, within the best horizontal connections. For instance, one European national CERT is attached to the Ministry of Finance – a ministry that has effectively nothing in common with the particular mission of a CERT as described by CERT/CC at Carnegie Mellon University.[363, 364] However, there are numerous examples where a government CERT will, for instance, not receive specific intelligence as it is not part of the right governmental information channel, even though they are often the only body that can actually act on this intelligence. This in turn limits the effectiveness of national-level CERTs, leading other departments to duplicate their activities which can ultimately lead to a 'function creep' with an inter-agency conflict as a result.

### 4.2.2. Across the Incident Management Cycle

A third method of delineation is to distinguish the cyber security functions, capabilities and responsibilities along the so-called 'incident management cycle'. The 'plan-resist-detect-respond'[365] security incident management cycle is one popular approach that has been specifically been adapted to information security.[366] This

---

362 Described within the present context as 'tactical' function, although, in fact, a CERT/CSIRT is essentially an 'organisational' unit with its own specific subordinate tasks (see Section 3.1.4). In essence, a CERT is group of people in an organisation who coordinate their response to breaches of information security or other computer emergencies such as breakdowns and disasters. Other accounts also refer here to a Computer Security Incident Response Team (CSIRT), a Computer Incident Response Team (CIRT) or just Incident Response Team (IRT). A CERT is a highly scalable entity: it can range in size from a single part-time employee without an assigned workstation to an organisation with hundreds of staff providing 24/7 services from a hardened facility.

363 See Carnegie Mellon University, 'About Us'.

364 Robert Bruce et al., International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues (TNO Report 33680), (Delft: Tuck School of Business at Dartmouth, 2005), http://www.ists.dartmouth.edu/library/158.pdf. vii, and 77-80.

365 Lenny Zeltser, 'The Big Picture of the Security Incident Cycle,' *Computer Forensics and Incident Response*, 27 September 2010.

366 See, for instance, NITRD, 'Interagency Working Group on Cyber Security and Information Assurance (CSIA IWG),' NITRD, https://connect.nitrd.gov/nitrdgroups/index.php?title=Interagency_Working_Group_on_Cyber_Security_and_Information_Assurance_%28CSIA_IWG%29.

cycle closely resembles the traditional emergency management cycle (comprising four elements: mitigation, preparedness, response and recovery), a cycle which is often found in the US emergency management literature and functional planning.[367]

In Europe, four or five elements are recognised in making up the cyber security incident management cycle: pro-action, prevention, preparation, response and recovery. Response and recovery are sometimes combined into a single element: suppression. Some nations, like the Netherlands, recognise another essential sixth element: aftercare/follow up.

The lack of a uniform structure for incident, emergency and crisis management is reflected by a wide variety of definitions for each of these elements in the security management cycle.[368, 369] For the decomposition approach this will not be a problem as, in this section, it is only needed to understand the functional placement of NCS functions, capabilities, and responsibilities along the incident response cycle.

**Pro-action**: defined as 'activities that reduce or remove the structural causes of insecurity.'[370] Pro-action comprises carrying out a national risk assessment (NRA) for the cyberspace domain, establishing a legal framework for cyber security, and an organisational framework. The NRA may identify insufficient and non-existing, but required, cyber security capabilities. It is up to the policy level to decide when this identified gap is filled (or not).

**Prevention:** in an emergency management context this has been defined as 'actions to avoid an incident or to intervene to stop an incident from occurring.'[371] For the purposes here, we use a slightly different definition: 'actions to prevent hazards from developing into incidents altogether or to reduce the effects of possible incidents'. Preventive cyber security measures reduce vulnerability to the global cyberspace and to individual NCS in particular.

**Preparation:** defined as 'planning, training and exercising' or as 'a continuous cycle of planning, organising, training, equipping, exercising, evaluating, and taking

---

367 See, for instance, Michael K. Lindell, Carla S. Prater, and Ronald W. Perry, Fundamentals of Emergency Management (Washington, DC: FEMA, 2006), http://training.fema.gov/EMIWeb/edu/fem.asp.

368 ICDRM, Emergency Management Glossary of Terms, (Washington, DC: George Washington University, 2010), http://www.gwu.edu/~icdrm/publications/PDF/GLOSSARY%20-%20Emergency%20Management%20ICDRM%2030%20JUNE%2010.pdf.

369 Dutch Ministry of Housing, Spatial Planning, and the Environment, Handreiking Security Management, (The Hague: Dutch Ministry of Housing, Spatial Planning and the Environment, 2008), http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2010/11/26/handreiking-security-management/11br2008g225-2008613-154851.pdf. 23.

370 Ibid.

371 ICDRM, *Emergency Management Glossary of Terms*. 76.

corrective action in an effort to ensure effective coordination during incident response.'[372]

**Response:** addresses the immediate and short-term effects, and prevents further damage after an incident occurs.[373]

**Recovery:** this encompasses 'activities and programs implemented during and after response that are designed to return the entity to its usual state or to a 'new normal'.'[374]

**Aftercare/follow up:** takes into account the psycho-sociological impact of an incident to (parts of) the population, covers incident and incident management investigation (such as fact finding and the writing of lessons identified), as well as forensic analysis, criminal investigation and the prosecution of suspects.

The security incident management cycle stems from an understanding that the lessons identified during the preparation (through aftercare/follow up) need to be converted into lessons learned.[375] These can subsequently either be adapted as a strategy and policy (pro-action), lay the foundation for new or revised prevention measures and approaches, help to develop and implement new or changed preparation measures (e.g., exercise programme), or can usefully be employed to implement and train changed procedures and processes that are part of the incident response element of the cycle.

Below, we will use this six elements model to discuss common and specific functions, capabilities and responsibilities at the national level.[376] The functions and capabilities placed in the six elements model can easily be mapped by the reader to one's national cyclic five or four elements model if required.

## 4.3. CYBER SECURITY STAKEHOLDERS

A wide range of stakeholders either provide or interact with cyber security functions, both at the national and international levels. These stakeholders are the same ones identified in the previous section: governmental, national/societal and

---

372 US Department of Homeland Security, National Incident Management System, (Washington, DC: FEMA, 2008), http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf. 145.

373 ICDRM, *Emergency Management Glossary of Terms*. 85-6.

374 Ibid., 82.

375 Note the distinction between 'lessons identified' and 'lessons learned'.

376 This 'operational' perspective includes the (inter)national functions, capabilities and responsibilities, and not at the tactical level of cyber security organisations which is internal to a department, agency, or other organisation.

international/transnational. Similar to what is described in the previous section, stakeholders are not necessarily constrained within each category but can operate with multiple 'hats'. For example, a government body may act as an end-user (Whole of Nation); help develope a digital certificate for service providers (Whole of System), and establish regulation (Whole of Government). Therefore, we use the following three non-exhaustive sets:

- Governmental:
  - the national government, its public and semi-public agencies,
  - independent regulatory bodies,
  - inspectorates dealing with cyber security aspects for their top-level domains,
  - the military, and
  - local government/administration & municipalities;
- National/Societal:
  - critical infrastructure (CI) sector organisations & operators,
  - ICT service providers (e.g., Internet Service Providers (ISP) & cloud services),
  - industry and businesses at large (and their branch organisations),
  - small and medium enterprises (SME),
  - (national) software and hardware manufacturers and system integrators,
  - universities and research & development organisations,
  - specialised defence and security contractors,
  - the population at large;
- International/Transnational:
  - multinational arrangements & bodies (e.g., G8, EU, OSCE,[377] ITU, World Bank, Europol, Interpol),
  - multi-stakeholder institutions (e.g., IGF,[378] ICANN[379]),

377 OSCE = Organisation for Security and Co-operation in Europe.

378 IGF = Internet Governance Forum.

379 ICANN = Internet Corporation for Assigned Names and Numbers.

- international standardisation bodies (e.g., FIRST, ISO[380]),
- informal international arrangements (e.g., IETF,[381] IEEE),
- key global infrastructure providers (e.g., backbone providers), and
- key global software and hardware manufacturers.

When discussing specific cyber security functions, capabilities and responsibilities in the following sub-sections, this list of stakeholders will be referred to when applicable.

## 4.4. MAIN FOCUS OF ANALYSIS

### 4.4.1. Along the Mandates

Figure 4 shows the generic model with the six elements of the cyber security cycle versus the five mandates as defined by Klimburg[382] and introduced in Section 1. The elements of the cyber security incident management cycle for each mandate which are not key at the national level are suppressed in the figure.

The internet governance/cyber diplomacy mandate acts across all of the incident cycle elements, such as international pro-active arrangements; harmonised prevention actions; exercises to be prepared for a hot phase response, and seeking international support during a hot response-recovery – follow up phase. The activities are mainly positioned at the policy/strategic levels.

The two areas of the cyber security crisis management and CIP mandate require a split. Cyber security crisis management requires a set of operational and tactical level functions for the preparation, response, recovery and aftercare/follow up elements of the incident response cycle, whereas the CIP strategic through tactical focus lies with prevention. The preparation through recovery elements are covered to mitigate the exposure in case prevention fails.

The military cyber operations mandate, above all, needs to protect its own cyber infrastructure. However, this is an internal organisational issue. At the national level, military cyber operational response and recovery capabilities need to be prepared (tactically and operationally) for countering cyber attacks against one's

380 ISO = International Organization for Standardization (www.iso.ch).

381 IETF = Internet Engineering Task Force – leads the internet protocol standardisation efforts.

382 See Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65)*.

nation. These capabilities may include both pre-emptive cyber strikes and (counter) attacks.

As part of their tasking, military cyber defence capabilities may be involved in the cyber protection of international alliances such as NATO and the EU. Currently, frameworks for collective military cyber defence operations do not exist or have not been made public. However, the Dutch government endorsed the view that:

> 'Under international law, the use of force in self-defence pursuant to Article 51 of the UN Charter is an exceptional measure that is justified in armed cyber attacks only when the threshold of cyber crime or espionage is breached. For a cyber attack to justify the right of self-defence, its consequences must be comparable with those of a conventional armed attack. If a cyber attack leads to a considerable number of fatalities or large-scale destruction of or damage to vital infrastructure, military platforms and installations or civil property, it must be equated with an 'armed attack'[383]

and:

> 'An organised cyber attack on essential state functions must be regarded as an 'armed attack' within the meaning of Article 51 of the UN Charter if it causes (or has the potential to cause) serious disruption to the functioning of the state or serious or prolonged consequences for the stability of the state, even if there is no physical damage or injury. In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks.'[384]

It concludes that 'Articles 4 and 5 of the North Atlantic Treaty may be applied to attacks in cyberspace. Article 5 is worded so generally that it can cover all forms of armed force. Article 4 is not as extensive in scope and may be applied to cyber attacks that endanger national security but do not breach the threshold of an armed attack.'[385] Therefore, collaborative cyber defence against a hostile actor causing a major cyber disruption to one or more nations of the Alliance is considered to be covered under the current North Atlantic Treaty.[386]

---

383 AIV/CAVV, Cyber Warfare, (The Hague: AIV, 2011), http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf.

384 Ibid.

385 Ibid.

386 For a further discussion on this, see Section 5.3.

The (counter-) intelligence mandate, first and foremost, focuses on prevention: the timely understanding plans and techniques of potential lone wolves, activists, terrorists, and adversary states. In case prevention fails, intelligence has to attribute attacks to specific attackers as part of response and follow up. Cyber security has been added as a new domain to the existing set of (counter-) intelligence activities which are mainly placed at the tactical/operational level. When applied, cyber security counter-intelligence is a preventing task by nature. However, the counter-intelligence capability may include offensive disruption tasks, when applicable.

The counter cyber crime mandate requires specific strategic and operational pro-action activities, and operational and tactical activities for all other elements.

**Figure 4:** The Five Mandates and the Six Elements of the Cyber Security Incident Cycle Model

### 4.4.2. Along the Cross-Mandates

In addition to the NCS mandates we also identified three cross-mandates. As is shown in Figure 5, the cyber security coordination cross-mandate crosses all of the five NCS mandates. At the political level this is synonymous with the overall coordination and control of NCS efforts. At the strategic and operational level it is primarily concerned with avoiding duplication of efforts, while at the tactical level it refers to the need to connect various tasks with each other.

The cyber security information exchange and data protection cross-mandate function has its main information exchange focus in prevention, response and recovery, and is active across all levels of activity. While at the tactical level it is important to exchange technical information on cyber threats, vulnerabilities and attacks, the sharing of intelligence at the very top of government and with private industry (e.g., critical infrastructure operators) when required, is no less important. However, most of the time, operational information exchange will occur during preparation and aftercare/follow up by specific organisations such as national crisis management and investigation organisations, respectively. Proper data protection processes are a pre-condition for operating cyber systems. The main focus is driven by the political/policy side, which must ensure the appropriate application of guidelines (OECD)[387] or legislation (e.g., within the EU[388]) across all forms of information exchange. This is supervised by Data Protection ('Privacy') Authorities[389] which keep the oversight as regulators at the operational level or working within the legal advisory frameworks of the relevant institutions (such as within the intelligence services). It is important to note that information that has been gathered in clear breaches of applicable data protection legislation can be sufficiently 'contaminated' that foreign partners may not want to use it – effectively depriving that respective nation of valuable diplomatic currency.

Cyber security research and development (R&D) and education (which includes awareness) form the third cross-mandate. Although each mandate may have its own R&D and education requirements and activities, cyber security awareness and education at the (inter)national level can effectively be organised across the five cyber security mandates to avoid duplication and waste of efforts. This cross-mandate capability will often be connected within an overall national and international R&D context (e.g., in researching internet security issues). Thus, it is primarily an (inter)national prevention capability. However, on the one hand

---

387 OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

388 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal, L 281.A new draft Directive is being worked on in 2012.

389 For example the Information and Privacy Commissioner in Ontario, Canada: www.ipc.on.ca.

it is also a very important 'pro-action' capability supporting efforts for national risk assessment. On the other hand, it includes the development of, for instance, awareness campaigns about cyber security for specific population groups.

**Figure 5:** The Cross-Mandates and the Six Elements of the Cyber Security Incident Cycle Model

## 4.5. THE FIVE MANDATES OF NATIONAL CYBER SECURITY

Based on the previous work of Klimburg[390] and using the combined model outlined above, it is possible to position the common and specific cyber security functions along specific mandates/cross-mandates and the cyber security incident management cycle (figures 4 and 5). Also, it is possible to distinguish common cyber security functions and capabilities at the national level from specific functions which may be needed and fit only specific nations.

Before discussing the figures in more detail, it should be remarked that this is the optimal, clean sheet positioning of the cyber security functions – a theoretical best practice. As discussed by Klaver et al.,[391] a nation shall keep in mind that its existing national (and international) organisational frameworks and the functional division between departments, agencies and public bodies gradually developed over a long period of time based on historic, cultural, legal, political and other reasons. In every nation there will be a number of specific local conditions that determine the current placement of functions and the course of existing institutions. Consequently,

---

390 Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65).*

391 See, for instance, Klaver, Luiijf, and Nieuwenhuijs, *The RECIPE Project: Good Practices Manual for CIP Policies. For Policy Makers in Europe.* 10-1.

a transposition of the theoretical best practice institution to a country's local conditions situation is certainly required.

### 4.5.1. Military Cyber Operations

The cyber security functions resident within the military domain differ from nation to nation, as the exact definition of military cyber operations will also differ. Overall, this mandate can include a very wide range of sub-mandates, not all of which will be applicable in every nation. Firstly, this includes 'cyber defence' – the protection of its own ICT systems, usually with a CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team) type of organisation in the lead and heavily dependent upon intelligence networks. Secondly, it can include options for strategic cyber operations – the ability to wage a 'cyber war' on the war fighting capability of the enemy.[392] Thirdly, it can include specific 'battlefield cyber capabilities' – those that are deployable within an operational and tactical battlefield environment (for instance against an enemy air defence system). Fourthly, it can include the modernisation efforts of more traditional military capabilities, such as those associated with Network Centric Warfare (NCW). It is important to note that the mandate may not only be national: a military cyber organisation may receive a mandate to support that nation's allies (e.g., within NATO) in an extension to its common security task. Apart from cyber defence (preparation, response and recovery), this may also include pre-emptive strike capabilities against a clear and present threat, counter-attack (response), or even an offensive capability mandate.

In case of a domestic national emergency, some nations have legal provisions for empowering the military to assist in emergency management, and help provide for internal security. Some of the military cyber security capabilities may, therefore, be trained to protect the 'homeland's cyberspace' in case the normal crisis response exhausts its resources to counter a cyber security crisis. The operational/tactical[393] command and control chain of the provided military cyber capability is, however, usually subordinate to the civil response authorities.[394]

Some nations (e.g., the United Kingdom and the Netherlands) organise their operational/tactical military cyber security response force in a flexible way. Others

---

392 See, for instance, Gregory Rattray and Jason Healey, 'Categorizing and Understanding Offensive Cyber Capabilities and Their Use,' in *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy*, ed. National Research Council (Washington, DC: The National Academies Press, 2010).

393 Note that the operational and tactical levels are reversed in the military structure as compared to civil structures.

394 France, the Netherlands and Switzerland are but three countries as an example.

(such as Estonia[395]) have created reservist or paramilitary cyber organisations that can provide reinforcement for regular military cyber forces in an emergency. These approaches are particularly useful given the inability of most nations to actually maintain all potentially required technical cyber skills in their organisation at all times.

### 4.5.2. Counter Cyber Crime

The counter cyber crime mandate comprises a wide set of organisations. At the policy and strategic levels, a ministry of justice is involved in the national, and often international, development and maintenance of cyber security legislation. Similarly, a ministry of the interior will often manage the dedicated police resources. Unlike in other mandates, however, some of these capabilities may well reside at a 'local' (provincial) governmental level, and not only be the responsibility of the central government.

Cyber crime prevention is a multi-angled issue. From the economic perspective, a ministry of economic affairs may manage cyber security awareness at the operational level and development programmes against cyber crime. Note that this overlaps with the R&D and education cross-mandate to be discussed later.

From the Whole of Government (WoG) perspective, state security and cyber crime prevention is an organisational issue across all government department and agencies. Currently, nations increasingly assign this strategic/operational responsibility to a Chief Information (Security) Officer (CIO or CISO) who has to develop, maintain and monitor government-wide information and cyber security policies.

From the perspective of secure service provisioning to the public at large, non-governmental service organisations such as ISPs may actively disrupt the spread of malware and other cyber crime activities. Public-private organisational arrangements such as an ISP Code of Practice and the identification of compromised customer systems exist in Australia,[396] and there are a number of anti cyber crime organisations that represent a mix of state and non-state actors.[397]

---

395 The Estonian 'Cyber Defence League' has, for instance, about 150 experts on call if necessary (see: Estonian Ministry of Foreign Affairs, 'Around 150 Experts Associated with Estonia's Cyber Defence League,' *Estonian Review*, 3 October 2011.).

396 Australian Attorney-General's Department, *Cyber Security Strategy*: 18-20.

397 One of these is, for instance, the Anti-Phishing Working Group (APWG). On a higher level, many of the top international network operators and similar technical experts regularly cooperate in a number of closed information exchange groups.

At the operational/tactical level, a police function is needed to investigate cyber crime, to try to take cyber criminals into custody, and have them prosecuted. This function extends across the preparation (training and exercises), response, and recovery elements. Logically, this function is embedded as a special knowledge area in the national police and local police forces. Cross-links and information exchanges with foreign police forces exist, either based on bilateral collaboration, or via the high-tech crime/cyber crime units of international police organisations such as Europol and Interpol.

To be effective, the police organisation may tie in with the national (and other) CERTs and public-private Information Sharing and Analysis Centres (ISACs) discussed under the cyber security crisis management & CIP mandate (Section 4.5.2). A common challenge is that, for many police forces, the act of starting a criminal investigation can put a sudden stop to information exchange that might help others. The public-private information exchanges and CERT organisations (Section 4.5.2) mostly deal with counter cyber crime prevention and response activities, and less often with the business continuity (or continuity of government) aspects managed under cyber security crisis management.

As part of the follow up, the national prosecution organisation has to extend and maintain its knowledge about cyber crime to operationally take care of the prosecution of cyber criminals as part of its normal way of operation. The forensic collection and analysis of data capability may (partially) be assigned to the police organisation. Some nations, however, have a national forensic service which covers, amongst other domains, the cyber security domain as well.

### 4.5.3. Intelligence/Counter-Intelligence

Distinguishing cyber espionage from cyber crime and military cyber activities is not uncontroversial. In fact, they all depend on similar vectors of attack and similar technology. In practice, however, serious espionage cases (both regarding intellectual property as well as government secrets) are in a class of their own. At the same time, it can be very difficult to ascertain for sure if the perpetrator is a state or a criminal group operating on behalf of a state, or indeed operating on its own.

Irrespective of who is actually behind the attack, cyber espionage probably represents the most damaging part of cyber crime (if included in the category). Lost intellectual property, for instance, was said to have cost the British economy £9.2 billion in 2011.[398] Cyber espionage, when directed toward states, also makes

[398] Michael Holden, 'Cyber crime costs UK $43.5 billion a year: study,' *Reuters*, 17 February 2011.

it necessary to develop specific foreign policy response mechanisms capable of dealing with the inherent ambiguity of actor nature in cyberspace. At the same time, counter-intelligence activities (e.g., detecting and combating the most sophisticated cyber intrusions) very often will depend upon other types of intelligence activity, including offensive intelligence collection but also extensive information sharing between international partners.

Collecting information through cyber means is just an extension of the existing set of capabilities being used by these services. Mostly, intelligence collected by other means will be used to address cyber security threats. The main focus is the defence of government systems from advanced cyber threats by state and non-state actors. Common tasks include information collection, verification, aggregation, analysis and dissemination.

Some nations allow their intelligence services to exploit the information for other purposes, or directly intervene in order to prevent threats from (re)occurring.[399] It is also possible that a specific vulnerability (and, therefore, an attack vector on a different organisation, such as a private company) will intentionally not be disclosed in order to further specific intelligence needs. Overall, intelligence and counter-intelligence organisations will concentrate their work within the operational/tactical environment but they will play an important role on the strategic level as well, especially in conducting regular threat assessments and the like. They are thus concentrated in the preparation and response phases.

### 4.5.4. Cyber Security Crisis Management and CIP

Cyber security crisis management comprises at least an operational and a mostly tactical function which spans the preparation (e.g., training & exercises), response, recovery, and aftercare/follow up elements of the cyber security incident management cycle. At the tactical level, a national computer emergency/security incident response team (CERT/CSIRT)[400] is required which preferably is fully linked to the national emergency/incident management structure at the political/strategic

---

399 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space.*

400 Bruce et al., *International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues (TNO Report 33680).* 112-3 and Appendix B.

level.[401, 402] Serious cyber incidents may lead to major disturbances and disruption of society. Incidents in, for instance, critical infrastructure sectors (such as energy and telecommunication) may have a serious impact at a national level when critical functions of cyberspace fail.[403] Moreover, the national emergency/incident management capability is closely connected to the national crisis communication capabilities, a function which comes in handy to communicate to the society and population about a serious cyber security incident at the (inter)national level.

At the operational level, there is often only a limited amount of integration due to legal reasons. For instance, in many nations there is a separation between the government CERT and the national CERT. The national CERT will often not be under direct control of the government, and will largely only have advisory functions. The government CERT does have (to various extents) operational control over the networks and network connections within its constituency, and is increasingly being used as the tactical level national cyber crisis management facility. Examples of such an arrangement can be found in Germany, the UK, the Netherlands, and many other countries.[404]

Different from cyber security crisis management, critical infrastructure protection (CIP) activities put their main focus on prevention. These are substantial governmental tasks, and a number of countries have set up dedicated CIP organisations, often with close connections to the internal security services.[405] This requires tools such as a national risk analysis[406] with perhaps corresponding national risk registries and regularly conducted assessments of specific risk factors

---

401 This means that the top crisis management advisory group (e.g., COBR in the UK) have NCS fully integrated into it.

402 It shall be noted that cyber-related emergencies with a serious national impact, but with different escalation characteristics, may occur more often than other emergencies. National cyber incidents may require a more flexible escalation process which may not require additional legal 'emergency' powers to deal with every single cyber-incident of national significance. To avoid a 'permenent state of emergency' it is necessary to re-conceptualise the tasks of 'national crisis management' to also include 'national incident management'. An equivalent level of emergency in another domain may be dealt with by a regional crisis centre, but the nature of cyber incidents at the national level may require the response of the national crisis response function.

403 For a concrete analysis of the economic effects of a major power outage, see: Public Safety and Emergency Preparedness Canada, Ontario – U.S. Power Outage – Impacts on Critical Infrastructure, (Ottawa: Public Safety Canada, 2006), http://www.publicsafety.gc.ca/prg/em/_fl/ont-us-power-e.pdf. More recently, an Austrian study was one of the few attempts to examine the consequences of a national blackout, see: Johannes Reichl and Michael Schmidthaler, Blackouts in Österreich Teil I – Analyse der Schadenskosten, Betroffenenstruktur und Wahrscheinlichkeiten großflächiger Stromausfälle, (Linz: Johannes Kepler Universität Linz, 2011), http://energyefficiency.at/web/projekte/blacko.html.

404 For a list of European CERTs and their constituents/stakeholders, see: ENISA, 'CERT Inventory,' ENISA, http://www.enisa.europa.eu/activities/cert/background/inv.

405 Examples of such organisations include the CPNI in the UK, and the CNPIC in Spain.

406 For a UK example, see: UK Cabinet Office, 'Risk Assessment,' UK Cabinet Office, http://www.cabinetoffice.gov.uk/content/risk-assessment.

to specific objects, organisations or processes/services. Secondly, it requires the development or adoption of information security standards or legislation within both the government and the private sector. Implementing information security practices[407] – perhaps the single the most basic and essential task within NCS – can be difficult to accomplish across central government, let alone the associated private sector critical infrastructure. Some countries simply proscribe the use of specific information security practices,[408] while some countries have more comprehensive legislation.[409] A third preventive tool, particularly for cyber security, is the information exchanges between the various actors. One approach[410] differentiates between three types of information exchanges. Firstly, a 'third party' model, which only involves exchanges between the non-state actors and without any government presence. Secondly, a 'community' model[411] that is usually sponsored by the government and security services, and provided with limited amounts of intelligence on threats, but not controlled by them. An example of this arrangement is provided by the UK Warning, Advice and Reporting Points (WARPs), or the Dutch Information Sharing and Analysis Centres (ISACs).[412] Finally, the 'hierarchical' model of information exchange is maintained by the government. It routinely delivers classified information to selected private organisations and companies. Examples of this arrangement can be found within France, Spain, the UK, the USA and a number of other countries. Particularly when these information exchanges are set up as public-private partnerships, they can further be connected internationally.[413] The national crisis management capability may be closely linked with the information exchanges. For all of these relationships, however, a considerable amount of trust between the various state and non-state actors is a necessary condition, and trust can only be built over time.[414]

---

407 For examples of approaches to information security, see Section 1.3.

408 For instance the German *Grundschutz* approach, or the French EBIOS tool.

409 One of the most extensive legislative examples is the 2002 US Federal Information Security Management Act (FISMA). FISMA is supported by a wide range of tools and services and aims to provide for standardised levels of information security across the civilian US federal government systems.

410 Sam Merrell, John Haller, and Philip Huff, Public-Private Partnerships: Essential for National Cyber Security [Transcript], (Pittsburgh, PA: Carnegie Mellon University, 2010), http://www.cert.org/podcast/show/20101130merrell.html. 5-7.

411 See, for instance, Austrian Federal Chancellery, *National ICT Security Strategy Austria*: 16.

412 See: WARP, 'WARP – Protecting our information infrastructures,' CPNI, http://www.warp.gov.uk. See also CPNI.NL, 'Werkwijze ISACs,' CPNI.NL, https://www.cpni.nl/informatieknooppunt/werkwijze-isacs.

413 An example of this is the European Public Private Partnership for Resilience (EP3R) maintained by the EU.

414 Klaver, Luiijf, and Nieuwenhuijs, *The RECIPE Project: Good Practices Manual for CIP Policies. For Policy Makers in Europe.* 10-11.

### 4.5.5. Internet Governance and Cyber Diplomacy

Internet governance[415] builds on an infrastructure of non-governmental driven self-regulation, in which the internet grew bottom-up with a minimum of government and public sector influence. Internet volunteers and experts organised themselves to drive the architectural and protocol development of the internet in self-organising structures such as the Internet Architecture Board (IAB) or the Internet Engineering Task Force (IETF). The internet-only part of cyber security is just one of the topics dealt with in internet governance but, despite different initiatives, no single organisational body drives the rate of progress on security issues.[416] The main activity areas are related to pro-action/prevention, including the standardisation of security options in protocols, the development of specially designed cyber security protocols, and describing and standardising good tactical/operational practices. ICANN is one of the most important organisations within internet governance, and is responsible for coordinating activities to secure the core functionality of the internet and the global routing and naming infrastructure. Increasingly, incident response to cyber attacks on the basic backbone infrastructure (in particular the routing protocols) may require a globally operating operational and a distributed tactical incident response, recovery and follow up capability. ICANN has made proposals for a type of global crisis management capability[417] and the ITU has made some suggestions along these lines as well.[418]

Cyber diplomacy[419, 420] is considered here to be the general formal state engagement of a nation's diplomatic processes in the overall theme of global cyber security. In particular, this refers to multilateral or bilateral activity aimed at managing state-to-state relationships in cyberspace. Within the context of the United Nations, for instance, the Group of Government Experts (GGE) have been working on issues of international law of armed conflict in cyberspace, and are currently drafting principles for norms and standards of acceptable state behaviour. In 2012, the OSCE started a process to specifically create 'Cyber Confidence Building Measures'. A large number of other initiatives exist, both hosted by international or

---

415 A definition of internet governance can be found in: WSIS, *Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E)* (Tunis: ITU, 2005). Para 34.

416 It is true that there have been several attempts to deal with cyber security issues within internet governance. However, despite the security activities performed by DNS-OARC, ICANN's Security and Stability Advisory Committee (SSAC), its DNS Security and Stability Analysis Working Group (DNSSA-WG), or the valuable inputs delivered by the annual Internet Governance Forum (IGF) and many others, it is not entirely clear where the organisational responsibilities overlap and where better coordination is needed.

417 In particular, the need to establish a global 'DNS-CERT' or similar.

418 Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65).* 25-6.

419 Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, 7.

420 Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65).* 18-9.

multilateral organisations (for instance, G8, OECD, etc.) or even stand-alone (such as the Meridian Group).[421] At the bilateral level, a number of 'major cyber nations' have conducted so-called Track 1.5 discussions on ways for reducing tensions in cyberspace. Cyber diplomacy is thus more equivalent to traditional diplomacy activities such as arms control and counter proliferation. Cyber diplomacy should not be equated with 'e-diplomacy', which is more concerned with the delivery of government messages using 'new media' – even though there might be important overlaps. For instance, in 2012, China[422] accused the US Embassy in Beijing of violating the Vienna Convention on Diplomatic Relations,[423] as the Embassy was 'automatically' broadcasting air quality for Beijing via Twitter.[424]

When it comes to designing structures for cyber diplomacy and internet governance, most nations find it difficult to assign specific responsibilities where they belong or take them away from where they have 'historically' been situated. For instance, internet governance – which is largely still totally separate from cyber diplomacy – is often dealt with by a ministry of economics or infrastructure, and is rarely involved in NCS issues. For many civil servants it can be difficult to perceive the larger picture within international cyber security, in particular, the view beyond their own department or mandate. This can often go hand-in-hand with a substantial lack of technical understanding. The challenge is particularly acute when dealing with 'bottom-up' internet governance organisations such as the IGF, IAB, IETF, IEEE and others – organisations that are still largely staffed by volunteers who often seem to speak a completely different language than government officials.

Moreover, government officials often lack insight into which of their national experts are playing key roles in the international organisations.[425] Although internet governance is perhaps the leading example of a topic requiring a Whole of System (WoS) coordination, it has proven to be very difficult for governments to adequately find their way in the existing 'multi-stakeholder' environment. As a consequence, there has been increasing governmental support for an 'intergovernmental' solution to internet governance (e.g., one in which the non-state sector would play only a supporting role). This is despite the stated claim of most liberal democracies to keep the internet 'free from government control'.

---

421 For a list of relevant organisations, see: US Government Accountability Office, Cyberspace. United States Faces Challenges in Addressing Global Cybersecurity and Governance, (Washington, DC: US Government Accountability Office, 2010), http://gao.gov/assets/310/308401.pdf.

422 Keith Bradsher, 'China Asks Other Nations Not to Release Its Air Data,' *New York Times*, 5 June 2012.

423 United Nations, *Vienna Convention on Diplomatic Relations* (Vienna: United Nations, 1961).

424 Jovan Kurbalija, 'Is tweeting a breach of diplomatic function?,' *DiploFoundation*, 14 June 2012.

425 Creating and maintaining a collective 'Who is who in cyberspace' directory across the government may be a solution to overcome this hurdle.

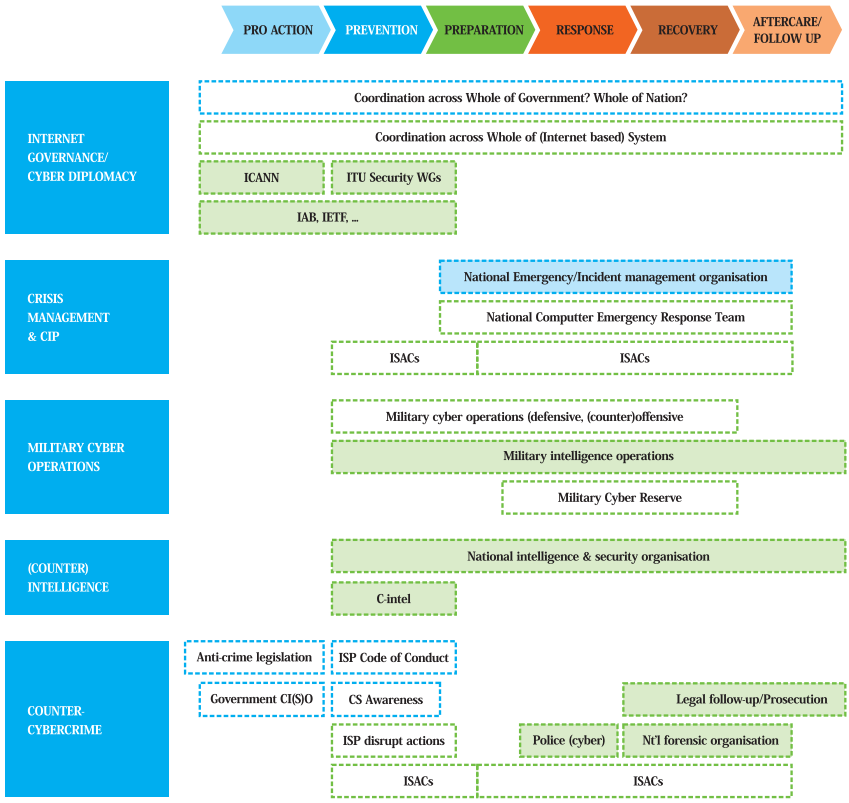


**Figure 6:** The Organisational Picture Across Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in existing organisation; dashed = option selected by some nations)

## 4.6. THE THREE CROSS-MANDATES ACTIVITIES

Besides the five specific types or mandates of national cyber security, there are also activities that apply to each of these mandates. Figure 7 shows the position of the organisations along the elements of the incident management cycle. Furthermore, the often complex relationships with international organisational structures will only be touched upon here briefly. They will be explained at length in Section 4.7.

### 4.6.1. Coordination

The cyber security coordination cross-mandate function is also seen as constituting national governance for cyber security. The coordination crosses the mandates discussed in Section 4.5 and spans the strategic, policy, and operational/tactical levels on the one hand, and all six elements of the incident management cycle on the other one. For a proper understanding, it shall be noted that the coordination concerns the wider understanding of cyberspace (or all ICT) and not just the internet[426] – unless a nation has specifically restricted itself to internet-connected ICT only in its NCS strategy (NCSS).[427]

In contrast to many other national security domains, cyber security crosses most of the classical governmental mandates. This requires a pro-active governance function within the national government which coordinates and spans the Whole of Government approach (WoG) and the full spectrum of the cyber security incident management cycle. The coordination responsibility is often assigned to a department responsible for more cross-departmental and agencies coordination activities (e.g., like the Cabinet Office or similar head of government functions).

This function will have a number of central roles. These include the coordination of a NCS risk assessment; the development and maintenance of a NCSS,[428] the alignment with the critical (information) infrastructure protection strategy (C(I)IP), and the possible establishment of a national (public-private) cyber security council.[429] Optimally, the same group will also play a decisive role in crisis management and any foreign security incidents involving cyber. A National (public-private) Cyber Security Council is meant to focus on pro-action, providing a well-balanced advice at the strategic level on cyber security issues and trends. However, during a major cyber security incident, crisis management may ask guidance from the Council. For that reason, the box in Figure 6 extends along all elements of the cyber security incident management cycle.

If a nation has developed and politically agreed on a NCSS, then it should set the policy outlines for the WoG. Each individual department may then develop strategies and policies for their own mandate, subordinate to the national policy and strategy. Moreover, the NCSS shall align with other national strategies and

---

426 Includes, for instance, process control systems, medical equipment, in-car systems, or RFID-chips.

427 Nations which, according to their NCSS, use an internet-only understanding of cyberspace are: Australia, Canada, Germany, Spain and New Zealand.

428 Eric Luiijf et al., 'Ten National Cyber Security Strategies: a Comparison,' in *Critical Information Infrastructure Security*, ed. Bernhard M. Hämmerli and Stephen D. Wolthusen (Springer-Verlag, forthcoming).

429 For example: Eijndhoven, 'Dutch Cyber Security Council Now Operational.'

policies, and recognise internationally agreed and nationally ratified cyber security treaties, legislation and regulations (e.g., those set by the EU and the Council of Europe Cybercrime Convention[430]). Optimally, the coordination body would supervise these developments.

Although a nationally coordinated approach and an internationally harmonised NCS legal framework would be preferred, most nations split the specific function of 'creation and maintenance of legal framework and regulation' across the various departments involved. For example, specific cyber security legislation and regulation regarding the telecommunication sector lies with a ministry of communications or economic affairs, whereas counter cyber crime legislation is supervised by a ministry of justice (or the like). The military task of establishing standard operation procedures and rules of engagement within the cyber domain is often dealt with purely within the military domain, and is seldom carried outside – with the possible consequence that the foreign ministry and the military/intelligence community might have a very different idea of what is 'legal' in cyberspace.

The most obvious governmental organisation to look after the international cyber security arrangements is a ministry of foreign affairs. However, given the spread of functions and responsibilities across the governmental mandates, often a specific ministry such as the ministries of economic affairs, telecommunications or health takes the lead. To avoid conflicts between departments and to harmonise the nation-wide approach, the ministry of foreign affairs is preferably in charge of the external cyber security policy coordination function, and draws on the other departments to provide factual expertise.

At the operational/tactical level, the coordination department, the intelligence community, or an interior ministry will be in charge of providing cyber security to the WoG, often under the responsibility of the government Chief Information Officer (CIO) or Chief Information Security Officer (CISO) (also see Section 4.5.5). Activities may, for instance, include awareness building; procedures and regulation for dealing with national secrets; standardisation of open source resources, and provision of, or oversight to, a government-wide digital signature infrastructure.

A separate, very specific, organisational function in the cyber security domain is the capability for an independent review of major cyber security incidents at the national level. By adding or contracting the right level of cyber expertise, this function can be embedded within an existing national incident review capability (e.g., a national safety and security board).[431] An example of such a review is the lessons identified

---

430 Council of Europe, *Convention on Cybercrime (ETS No. 185)*.

431 See, for instance, The Dutch Safety Board, http://www.onderzoeksraad.nl/en.

study[432] about the Dutch DigiNotar case, where the digital certificate provider for the Dutch government, its agencies, towns and municipalities and a number of private companies, was compromised.

### 4.6.2. Information Exchange and Data Protection

Few activities are as central to national cyber security as information exchange and data protection. The information exchange and data protection cross-mandate has its main focus on prevention, response, and recovery. The cross-mandate is mainly of operational/tactical nature. However, tactical information exchanges will occur during preparation and aftercare/follow up by specific organisations, such as national crisis management organisations and investigation organisations respectively. Data protection may be a consideration at the political/policy and strategic levels when considering new laws and cyber functions for society.

Information exchange[433] on cyber security information builds upon trust and value between two or more organisations and, sometimes, is even limited to mutual trust between persons only. Information sharing should not be confused with information provisioning, where an organisation is required by law or its mandate to provide (processed) information one-way to other parties, subject to relevant data protection requirements. Key to information sharing is the two way value-adding exchange of information on cyber security while balancing transparency and secrecy. Globally, the information age requires a need-to-share recognition balanced with trust and tempered by the need-to-know paradigm of information assurance. Cyber security information to be shared may include weak signals, incident data, threats, risk, security measures, coordinated defensive responses, tactical/operational experiences and good practices.[434]

Information sharing takes place within national and international communities that have a specific objective within the same mandate. This can include information exchanges between communities in alike mandates in different nations; international exchanges such as the European SCADA Security Information Exchange (EuroSCSIE); the European Financial Services Information Security Analysis Centre (FS-ISAC), and the Club de Berne (intelligence community), or between different communities in different national and international mandates such as critical infrastructure operators, police, and intelligence and security services.

---

[432] The Dutch Safety Board, The DigiNotar Incident: Why digital safety fails to attract enough attention from public administration, (The Hague: Dutch Safety Board, 2012), http://www.onderzoeksraad.nl/docs/rapporten/Rapport_Diginotar_EN_summary.pdf.

[433] Klaver, Luiijf, and Nieuwenhuijs, *The RECIPE Project: Good Practices Manual for CIP Policies. For Policy Makers in Europe.* 51-60.

[434] Ibid., 52.

### 4.6.3. Research & Development and Education

Typically, nations envision economic prosperity from information and communication technologies in their NCSS.[435] Nations often assign their strategic/operational level responsibility for stimulating innovation and economic development of cyber security R&D to their ministry of economic affairs. The strategic/operational management level aspects of the academic, often more fundamental, cyber security research efforts are managed by a ministry of science/education, in a number of cases in close coordination with a ministry of economic affairs and the more security-orientated ministries. The actual R&D programmes are managed at the tactical/operational level either by existing national organisations which manage R&D programmes in a wide set of research domains, such as companies or universities, or by specifically established organisations. A specific, academic-based organisation may be established which assists in the analysis and identification of lessons about the government response to a major cyber crisis.

By nature, R&D efforts are often prevention activities. This is notwithstanding the fact that these efforts include the R&D on support methodologies and measures for the preparation, response and recovery elements of the cyber security crisis management, military cyber operations, and counter cyber crime mandates. It can also include in-depth research into cyber attacks and their consequences that could potentially be used in more offensive activities.

Cyber security at the national level will fail when there is an inappropriate level of cyber security awareness and education. A nation requires its ministry of education and/or science to develop strategic/operational programmes for cyber security awareness and education. The base level programmes need to span a wide range of stakeholders: children at primary and secondary school, and a base level of awareness for adults and elderly people. Some of these programmes, however, may be organised and paid for by private industry (e.g., an anti-phishing TV campaign by financial institutions). It is, however, beneficial at the national level to orchestrate operational activities in order to avoid the duplication of efforts.

Apart from the general population and specific target groups within the population, a cyber security educational structure is required to assure that a sufficient number of cyber security experts and professionals are educated (and re-educated) to support all the cyber security activities outlined above, as well as in organisations outside the critical sectors and government.

At least as important as basic education is awareness raising among key decision-makers in both state and non-state organisations as to the extent of the cyber

[435] Luiijf, Besseling, and Graaf, 'Nineteen National Cyber Security Strategies.'

security challenge. This is particularly acute as the complexity and sometimes esoteric nature of the subject prevents a 'natural' education of these decision-makers over time. At the same time, the plurality of actors in cyber security means that especially the cooperation of non-state decision-makers is absolutely crucial in any NCSS – and this cooperation often will only occur when those decision-makers are fully aware of the extent of the challenge.

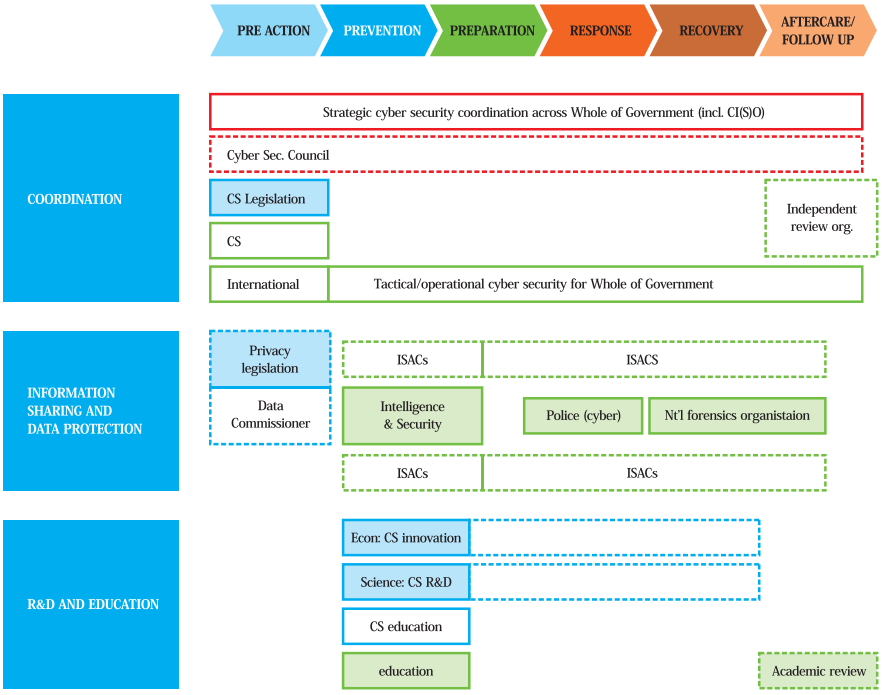


**Figure 7:** The Organisational Picture of the Cross-Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in existing organisation; dashed = option selected by some nations)

## 4.7. INTERNATIONAL CYBER SECURITY ORGANISATIONS

International organisations play a key role in cyber security, although they often only receive passing mention in NCSS. These NCSS will highlight the importance of international cooperation, and mention a few of the most prominent international organisations but often with a lack of detail of how or why these organisations are

important. First and foremost, NCSS deal with the international spectrum primarily as a WoG and, to a lesser extent, as a Whole of Nation (WoN) matter. Whole of System (WoS) approaches, when not government focused (such as within an international organisation), are much more difficult for national governments to conceptually deal with. These groups however represent a good share of international cyber security activity (in particular at the technical/operational level), which means that government consistently has trouble engaging to its full potential.

### 4.7.1. Government-Focused Activities

As mentioned earlier, the Whole of Government approach (also known in the UK as 'joined-up government' and the US as 'networked government') was originated to save costs and improve coordination. When discussing international organisations, WoG is being used here to discuss international cooperation between governments that generally exclude the private sector or civil society. These organisations tend to focus on the internet governance and cyber diplomacy, although much more emphasis is laid on the latter than the former.

The governments of the United States, Japan and the United Kingdom provide good examples of organisations which coordinate all international aspects of cyber security. The US has an appointed US Cyber Coordinator (in the White House National Security Staff), Japan has its own National Information Security Center and the UK has established the Office of Cyber Security and Information Assurance (with the two latter organisations being attached to their respective Cabinet Offices). These offices have senior people in (generally) sufficient numbers to coordinate other government ministries and departments. Often, the members of these offices are actual detailees seconded from those ministries, which aids speedy coordination. For instance, the UK International Cyber Policy Unit (ICPU) is located within the Foreign and Commonwealth Office but is largely staffed with individuals 'double-hatted' from the Cabinet Office. While the ministries of foreign affairs will have the functional lead, these central coordination groups have a strong role to play. In the United States, for instance, it was the National Security Staff, not the State Department, which led the writing and coordination of the International Strategy for Cyberspace.

WoG international activity solutions are often concentrated within bilateral agreements (i.e., cyber diplomacy), although there is a growing number of engagements inside intergovernmental forums. Bilaterally, there have been several important recent agreements. For example, India has signed cyber security

agreements with both the United States[436] and Japan.[437] To extend the extensive cyber security partnerships of the USA and the UK, the White House announced early 2012 that, 'President Obama and Prime Minister Cameron reaffirmed the vital partnership between [their] two nations on cybersecurity,'[438] and enumerated six specific areas of progress.

State to state agreements (outside of larger multilateral groupings) were originally relatively rare but, are rapidly increasing as an option for states,[439] such as when 'the United States and the United Kingdom [...] launched a trilateral initiative with Australia to fund new R&D for improved cybersecurity.'[440] Some agreements also already exist to facilitate cyber crisis management cooperation: a good example for this is the 'China-Japan-Korea (CJK) agreement.'[441]

These bilateral and multilateral agreements typically do not lead to the creation of new organisations to shepherd the agreed upon actions. They rather lead to increased cooperation between existing organisations, especially CERTs and ministries of defence and justice/the interior.

Cyber security agreements through intergovernmental organisations rely on the existing staff and bureaucracies of those groups. The most important tend to be long standing groups created to coordinate traditional national security and diplomatic issues. In 2012, the United Nations will be hosting the third meeting of the Group of Government Experts (GGE), organised by the Office of Disarmament Affairs, to discuss cyber norms.[442] China, Russia and other nations have issued a draft Code of Conduct calling for cyber norms, based on work done previously with the Shanghai Cooperation Organisation.[443] Meanwhile, the UN's ITU is often perceived to be striving to 'wrest control' over the internet from ICANN.[444]

Cyber issues have been on the NATO agenda for some time. Unlike other international organisations, this military alliance has extensive cyber systems which need to

---

436 US Department of Homeland Security, 'United States and India Sign Cybersecurity Agreement,' *Office of the Press Secretary*, 19 July 2011.

437 TNN, 'India and Japan agree to boost maritime, cyber security,' *The Times of India*, 1 May 2012.

438 White House, 'Joint Fact Sheet: U.S.-UK Progress Towards a Freer and More Secure Cyberspace,' *Office of the Press Secretary*, 14 March 2012.

439 See Section 5.3. for a discussion on non-NATO nation cooperation.

440 White House, 'Joint Fact Sheet: U.S.-UK Progress Towards a Freer and More Secure Cyberspace.'

441 English.news.cn, 'China, ROK, Japan pledge future-oriented partnership amid trilateral summit: joint declaration,' *English.news.cn*, 14 May 2012.

442 UNODA, 'Developments in the field of information and telecommunications in the context of international security,' United Nations, http://www.un.org/disarmament/topics/informationsecurity.

443 Jason Healey, 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms,' *New Atlanticist*, 21 September 2011.

444 See for instance http://www.bbc.com/news/technology-19106420.

interconnect with its many members during military operations. Accordingly, most of NATO's recent initiatives have been aimed at improving the cyber security posture of its own systems and it has a more pronounced focus on the mandate for military cyber defence operations than other international groups.[445]

There are some other international groupings that are customised just to deal with cyber (and other information protection) issues. Meridian is perhaps the most well-known. Since 2006, a programme committee comprised of international governmental organisations organises the annual event and develops the agenda (such as the Department of Homeland Security of the United States or the Infocomm Development Authority of Singapore).[446]

### 4.7.2. Nation-Focused Activities

The Whole of Nation approach, as mentioned earlier, includes a mix of government, private sector and civil society. Compared to government and internationally-focused organisation, WoN groups are the least difficult to categorise in the international sphere, although these non-governmental actors account for the bulk of what is termed 'national' cyber security, with a heavy focus on the mandates of crisis management and CIP. In international cyber security, WoN is used to describe where governments work closely with non-government groups, while still retaining a substantial voice, such as within the 'Organisation of Islamic Cooperation – Computer Emergency Response Team' (OIC-CERT).

The OIC-CERT is a grouping of organisations from Islamic nations to 'explore and to develop collaborative initiatives and possible partnerships in matters pertaining to cyber security.'[447] While it is open to membership from academia, companies and individuals, the group reserves full membership (and voting rights) only to governments.

A completely different example comes from recent collaborative *ad hoc* actions against networks of malicious computers called botnets. These 'take downs' were led by companies in the private sector but relied upon the coercive power of national justice systems. Microsoft has become especially well known for using this innovative tactic: teaming with other companies with knowledge of a particularly vicious (or vulnerable) botnet and then filing suit in court against the botnet's organisers. Using this authority, Microsoft and its partners, 'escorted by the U.S. Marshals – successfully executed a coordinated physical seizure of command and

---

445 Jason Healey and Leendert van Bochoven, 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow,' *Atlantic Council Issue Brief*, February 2012.

446 Meridian, 'The Meridian Process,' Meridian 2007, http://www.meridian2007.org.

447 OIC-CERT, 'Mission Statement' OIC-CERT, www.oic-cert.net.

control servers in two hosting locations to seize and preserve valuable data and virtual evidence from the botnets for the case.'[448]

### 4.7.3. System-Focused Activities

In the Whole of System approach there is cooperation among 'like-minded actors.' The government does not necessarily have any privileged position in the group. As in WoN, these WoS groups tend to keep a heavy focus on the mandates of counter cyber crime, crisis management and CIP. Despite the wide scope for effective and agile action of these non-state groups, they are often overlooked by NCSS.

One of the most important WoS organisations has already been discussed earlier. ICANN embraces a multi-stakeholder approach, so governments have a voice, but so do technical experts from the private sector and civil society.

The importance of WoS groups cannot be overestimated. For example, during the 2007 cyber attacks against Estonia, private sector members of NSP-SEC (Network Service Provider Security), a leading cyber attack mitigation coordination body of internet network professionals 'went to the EE-CERT [the Estonian CERT] to act as the liaison and to help the [Estonian] EE-CERT coordinate with CERTs and internet service providers in other countries to stem the attacks.'[449] The support for Estonia came not from NATO or other governments but through a non-governmental group.

Getting vetted into NSP-SEC is especially difficult as, once you are in, you have a positive obligation to stop any attack traffic traversing your network as soon as you are notified by another member of the group, no questions asked. As Bill Woodcock summarised it: 'If something needs to be taken down, it needs to be taken down and there isn't time for argument and that's understood up front, so there isn't a mechanism for arguing about it. You can argue about it later.'[450]

While NSP-SEC only operates in the phase of incident response, there are numerous other groups that cover other parts of the spectrum. For example, since 1990, the Forum of Incident Response and Security Teams (FIRST) has been 'an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.'[451] As with NSP-SEC, governments are members but have no privileged status.

---

448 Jeffrey Meisner, 'Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets,' *The Official Microsoft Blog*, 25 March 2012.

449 Jason Healey et al., Building a Secure Cyber Future: Attacks on Estonia, Five Years On [Transcript], (Washington, DC: Atlantic Council, 2012), http://www.acus.org/event/building-secure-cyber-future-attacks-estonia-five-years/transcript.

450 Ibid.

451 FIRST, 'FIRST Vision and Mission Statement,' FIRST, http://www.first.org/about/mission.

FIRST is one of the founding blocks of the CERT community.[452] Derived directly from the first worldwide CERTs and managed from a university, FIRST is essentially the most important certification body for any organisation or government seeking to be part of the worldwide CERT community. Members are able to collaborate with like-minded members across the entire spectrum of cyber security actions. FIRST working groups develop a whole range of tools, processes and products which are usually freely available.[453]

NSP-SEC and FIRST are long-standing groups, but other WoS organisations are *ad hoc* creations for a single purpose. Also known as 'Security Trust Networks',[454] these groups are often volunteer based, and concentrate a lot of operational or research capability within a completely informal network. Led by Microsoft, the Conficker Working Group was 'a collaborative effort with technology industry leaders and academia to implement a coordinated, global approach to combating the Conficker worm,' a particularly virulent piece of malicious software.[455] Even though these like-minded groups are at the forefront of much of cyber security, especially incident response, governments typically have little understanding of them or how to aid or even make room for them. For example, after battling Conficker, members of the working group said they' saw little participation from the government,' indeed even 'zero involvement, zero activity, zero knowledge.'[456]

There are, of course, active government-only international cyber security groups (e.g., the European Government CERT Group is a vital organisation within European cyber security), but most international cyber security groups are still non-state. Recognising the importance of these WoN and WoS groups in NCSS is an important step to improving security. Understanding the importance of non-state groups is, however, absolutely essential.

---

452 Bruce et al., *International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues (TNO Report 33680)*. 77-80.

453 FIRST, 'FIRST Vision and Mission Statement.'

454 Klimburg, 'Whole-of-Nation Cyber Security.'

455 Conficker Working Group, 'Announcement of Working Group,' Conficker Working Group, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/FAQ#toc6.

456 The Rendon Group, Conficker Working Group: Lessons Learned, (Washington, DC: Conficker Working Group, 2011), http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf. 34.

## 4.8. ORGANISATIONAL PITFALLS, FRICTIONS AND LESSONS IDENTIFIED

As some nations concentrate their cyber security on internet-connected systems only, a wide open gate is left for cyber crime in the other parts of cyberspace. A wide organisational understanding of cyberspace is needed to avoid organisational failure at the national level.

**Leaving a policy vacuum:** one pitfall is that nations unintentionally may leave a strategic and/or operational level vacuum around tactical capabilities – in other words, may create a 'labelled' department bereft of basic expertise or tasks, and without a top-level strategic vision. This vacuum will progressively fill itself due to function creep both vertically and horizontally,[457] leading to friction with other public and private organisations, and could also lack proper accountability.

**Allowing stovepipes:** cyber security is a global issue which crosses all governmental mandates, departments and agencies. There are many chances for the departments to engage in 'cyber empire building', using 'stovepiped' domains such as telecommunications, security, energy, health and economic innovation to overtly focus resources, legislation and regulations – detrimental to the exclusion of other issues. Moreover, the bureaucratic reality is that, in most nations, the cyber security subject areas are kept separate from each other in distinct mandates, often with their own definitions, emphasis and official slang.[458] The risk is very high that a strong stovepiped approach will lead to a set of uncoordinated, even overlapping activities and miscommunication. It will confuse private organisations which are faced with conflicting laws and regulation. For instance, cyber security breach notification obligations may be in conflict with privacy legislation, financial oversight or stock exchange rules. A strong coordination across the Whole of Government and strong public-private arrangements may help to avoid that situation. Even better is to link existing organisational structures together in a matrix structure – an effective and efficient way of building connectivity across governmental 'stovepipes', across public-private partnerships, and across trans-border networks.

**Drafting obsolete legislation:** another pitfall noticed in many of the current NCS approaches, is the organisational lack of governmental structures to prepare for new cyber threats and new ICT innovations. The rate of change in cyberspace means that organisations are constantly challanged by the need to modfiy

---

457 An incident response function like a CERT shall be focused on incident response and recovery. Some form of preparation is required. However, when such a CERT lacks a proper strategic/operational embedding, function creep may occur towards, for instance, pro-action and prevention aspects of critical infrastructure protection, and the area of cyber security policy development for its constituency.

458 See Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65)*.

stovepiped services and legislation.[459] As a result, cyber security legislation covers the digital crimes known from the past and do not embrace new ones. In particular, fundamental elements of cyber security – especially the need to concentrate on the obligation of the defender to adequately secure his systems rather than only trying to pursue a most often unknown attacker – have often not been appreciated by lawmakers.

**Lack of flexible cooperation:** apart from the WoG angle, new non-state organisations are constantly emerging whose work is relevant to NCS. Either in prevention or in the response/recovery/follow up phases, these new organisations often deal with cyber security issues in a bottom-up mode. They often find their existence in new types of community arrangements with minimum or even no government influence. The ability to flexibly work with these non-state organisations is thus an important part of future national cyber security.

**Unclear Information Exchanges:** when it comes to information exchange, unfortunately, many governments just know they want it. However, often they only have little knowledge about the actual goal of sharing or coordinating information between departments, let alone with international and/or non-state actors. Accordingly, companies in one CIP sector may get overlapping or competing requests to share information from ministries of the interior, justice or defence, from military services or commands, as well as functional ministries (such as financial regulators) and a cabinet office. This threatens to undermine the entire purpose of an information exchange, and can make a critical operational function into an organisational burden.

**Tolerating Cyber-Illiteracy:** another gap identified is the understanding of cyber security issues and 'language' by higher level public officials, decision-makers, judges and politicians. No standard and base level education training has been identified for those key individuals. The lack thereof causes misunderstanding, adverse decision-taking, imbalanced sentencing, and neglect of serious threats and incidents.

---

[459] Luiijf, Besseling, and Graaf, 'Nineteen National Cyber Security Strategies,' 23.

## Internet Governance and Cyber Diplomacy

The UK Foreign and Commonwealth Office (FCO) was one of the first foreign ministries to dedicate staff to coordinating and addressing the international aspects of cyber issues. Previously under the auspices of the FCO Director for Intelligence and National Security, the FCO dedicated resources from 2011, building up to a full team in 2012, in the newly-formed International Cyber Policy Unit (ICPU). ICPU staff are either from the FCO or the Cabinet Office for Cyber Security and Information Assurance (OCSIA). Its Director is double-hatted for FCO and the Cabinet Office. The ICPU is well-resourced – relatively speaking, no other NATO nation has committed a similar level of staffing to addressing international cyber issues. It leads and coordinates the UK engagement on international, multilateral and bilateral cyber diplomacy issues. These range from discussions on confidence building measures and norms of state behaviour to the economic and social benefits of cyberspace, while bilateral issues can also include transparency building to various degrees of operational cooperation.

ICPU works closely with the full range of UK government departments engaged in cyber issues from UK Department on Culture Media and Sport on internet governance issues, to the Home Office on cyber crime. Within the international multi-stakeholder context, ICPU has the oversight of the UK government position and supports other government departments where these are in the lead. Each UK government department has its own well defined role to play but OCSIA takes responsibility for ensuring delivery of the national cyber security strategy through coordinating government policy on cyber.

## Crisis Management and Critical Infrastructure Protection

The *Centre Opérationnel de la Sécurité des Systèmes d'Information* (COSSI) is the primary cyber defence organisation of the French government, and operationally responsible for managing national cyber crisis incidents. As part of ANSSI (a dedicated agency responsible for government information security within the Defence and National Security Department), COSSI is responsible for collating intelligence related to cyber threats both for the French government as well as for some of the critical infrastructure providers. COSSI is responsible for implementing many of the regulations and emergency ordinances of PIRANET, the French national cyber crisis management plan. In this context, COSSI depends mostly on CEVECS, a situational analysis and early warning centre that draws data from a wide array of feeds, and which has a 24/7 watch & warning component. The technical component of COSSI is mostly met by CERTA, the French government CERT, which receives technical alert information through a number of systems. At higher PIRANET alert levels, CERTA and CEVECS can be substantially reinforced with other personnel from the national security and defence ministry..

## Military Cyber Operations

The US military was probably one the very first militaries to have cyber units. The first such unit was the 609th Information Warfare Squadron of the US Air Force, which was stood up in 1996. The unit had both offensive and defensive capabilities that were to directly able to support combat operations.[460] In 1998 the Department of Defense (DoD) created the first joint cyber command – commanded by a two-star general – with the authority to order, rather than just coordinate, military defences. Within two years, the Joint Task Force on Computer Network Defense (JTF-CND) was also assigned the cyber offense mission, although this was re-assigned to another command a few years later when the JTF was given authority over, not just global network defence, but operations as well.[461] JTF-CND retained this responsibility until 2010.

In the intermediate period, a great number of cyber organisations proliferated across the DoD and the US National Security Agency (NSA – a DoD subordinate agency). It was to streamline all these various organisations into one command that the US Cyber Command (USCYBERCOM) was stood-up in 2010. As a major shake-up of the US military in cyber, USCYBERCOM was designed to overcome a large number of 'stovepiped' conflicts within the DoD. Henceforth, the activities of all four branches of the armed forces would be communicated, coordinated and, in part, directly controlled by USCYBERCOM. As a subordinate of US Strategic Command, USCYBERCOM is also the top-level organisation with final responsibility for DoD-related cyber offensive and defensive activity. A major novelty of USCYBERCOM was its collocation within the NSA and the 'double hatting' of its commander as also the director of the NSA. Besides the obvious resource benefits that this relationship provided, it also addressed a number of significant operational concerns, particularly with regard to the difference between espionage and warfare. In 2011, the official USCYBERCOM budget was over $3.2 billion, but this did not take into account supporting budgets within the NSA or other aligned structures and commands.

460 Jason Healey and Karl Grindal, 'Lessons from the First Cyber Commanders,' *New Atlanticist*, 14 March 2012.

461 Ibid.

## Intelligence and counter-intelligence

Sweden maintains one of the most advanced Signal Intelligence (SIGINT) systems in Europe, operated by the National Defence Radio Establishment (FRA). With wide authority to tap foreign voice and data communications crossing its territory, FRA also operates under very close (and very transparent) supervision by specially appointed legal bodies. No data inspection may be conducted by the FRA without a specific request being issued by the Swedish Defence Intelligence Court – a body specially set up 2009 to protect 'personal integrity' in cases of surveillance. The Court also controls the search criteria and other provisions to limit the amount of accidental surveillance that may occur, and an independent 'Integrity Ombudsman' further shadows the work of the Court. Institutional oversight of the Court itself is provided by a separate judicial body, SIUN, which is also able to directly investigate intelligence activities of the Armed Forces. SIUN can also initiate investigations upon request of private persons.

## Counter Cyber Crime

Brazil has been confronted with one of the fastest growing local cyber crime populations in the world. Increasingly, these cyber criminals are not only internationally active, but also pose a serious threat to Brazilian internet users as well. Consequently, in recent years the Brazilian Federal Police has greatly invested in counter cyber-crime resources, increasing both the ability to undertake network investigations as well as conduct (hardware) forensic analysis. Two units were especially emphasised – the centralised Cybercrime Suppression Unit (URCC), and the Computer Forensics Unit (CFU). The forensic specialists are particularly intended to support investigations of the URCC by being able to quickly and reliably respond to local investigations across the territory of Brazil. The CFU, which has been active since 1996, has a headquarters unit with around 24 specialists, but mostly operates through some 180 forensic specialists in about 50 field offices. A highly flexible pay structure has allowed the Federal Police to offer forensic specialists and others very high salaries, leading to a high standard of recruitment.

# 5. COMMITMENTS, MECHANISMS & GOVERNANCE

*Victoria Ekstedt, Tom Parkhouse, Dave Clemente*

**Section 5: Principal Findings**

- The national and international legal environment brings with it a large set of pre-existing commitments (e.g., treaties) that constrain the freedom of domestic policy-makers.
- A consensus is emerging that International Humanitarian Law can be applied to cyber conflict, and that a cyber attack could potentially rise to the level of an 'armed attack.' Human Rights are also increasingly being interpreted as being applicable to cyberspace.
- The Convention on Cybercrime is currently one of the most relevant international frameworks. In particular, Articles 23-34 make very specific demands to the level and type of international cooperation (for instance 24/7 point of contact) that need to be considered when designing national cyber security policies.
- All national cyber security policies should be connected to relevant Information Security Management architectures. Without such a link there can be no NCS.
- NATO has increased its focus on cyber security and is increasingly cooperating with non-NATO nations, the EU and International Organisations as well. This provides an additional planning framework with which to adjust localised, national structures.

## 5.1. INTRODUCTION

In many ways, the development of national cyber security (NCS) policy faces challenges both known and unknown. There are a host of familiar obstacles – political, bureaucratic and financial (both national and international) – as well as relatively new and unfamiliar obstacles, such as the power of the private sector in cyberspace, a rapidly shifting landscape and the gradual, yet inexorable, expansion

of this man-made domain. Growing societal dependence on this complex and entirely man-made environment produces risks that are often opaque and poorly understood. In addition, understanding how the cyber domain does or does not integrate into the domains of land, air, sea and space is a persistent challenge. Yet the potential opportunities – the myriad choices – presented by cyberspace are too lucrative for society to significantly curb its growing dependence on digital technologies. New frameworks and policies are needed to cope more effectively with the challenges that are emerging.

At the **political level** the challenges of cyber policy development may look familiar. While there may be new mandates and resources to be negotiated, their allocation conforms to political processes that are well understood by those vying for power. There are entrenched interests and prior commitments (both national and international) that must be navigated. These and many other cyber policy challenges conform – to a greater or lesser degree – to the political challenges inherent to policy development in most arenas.

At the **strategic/operational level**, some governments may choose to centralise the majority of decision-making powers, while others may devolve this to a lower level according to a particular need (e.g., to build resilience and responsiveness into highly decentralised and mostly privately-owned critical infrastructure). Although most nations will likely see a need for the development of cyber security policies at the central government level, in order to do this it may be necessary to create new offices to respond to cyber-specific requirements.[462] Not every nation will consider a US-style Cyber Command to be the most appropriate model to emulate, and indeed few can match the resources available to the US Government.[463] Resource constraints are always a consideration, yet financial pressures are no excuse for poorly conceived policy. Indeed, drowning a problem in money is a rarely good option and is also unlikely to produce sustainable policies.

The **national and international legal environment** brings with it a host of pre-existing commitments (e.g., treaties) that constrain the freedom of domestic policy-makers. Commercial law and the international economic environment will also influence the creation and constrains of domestic cyber security policies. In large part, commercial constraints on policy-making are a natural result of privately owned infrastructure, particularly critical infrastructure, over which a government may have limited influence.

---

462 For example, the UK Office of Cyber Security and Information Assurance (see: UK Cabinet Office, 'Office of Cyber Security and Information Assurance (OCSIA),' http://www.cabinetoffice.gov.uk/content/office-cyber-security-and-information-assurance-ocsia.).

463 Wesley R. Andrues, 'What U.S. Cyber Command Must Do,' *Joint Forces Quarterly* 4, no. 59 (2010).

This section describes some of the various frameworks and mechanisms that governments may need to consider as they develop cyber security policies. The sum of these tools is too numerous for any single publication to address and this section pays attention only to the most important ones. It notes the utility (or otherwise) of existing tools and identifies existing and emerging gaps in the policy landscape. This section is divided into three sub-sections. Section 5.1 analyses the nature of state commitments – legal commitments in particular – and the impact they have on the development of national cyber policies. Section 5.2 examines the practical interpretation of these commitments and tackles questions about how they can be governed and improved. Finally, Section 5.3 looks at NATO's cyber position, in particular its practical activities and engagement with the EU.

Throughout this section, the general features of all commitments and tools are described, while providing sufficient information for more detailed enquiries to be made where desired. Attention is given to the flexibility and applicability of existing laws and frameworks as well as their relative pros and cons, levels of commitment, potential political returns on investment, and practical security advantages. Thought is given to tensions between national and international mechanisms and the difficulty these tensions generate for domestic cyber policy development. This section also builds on several primary themes, which are acknowledged for the sake of clarity and as a necessary courtesy to the reader.

Firstly, policy development is inherently about trade-offs: long-term vs. short-term, lavish vs. frugal, and expansive vs. limited. It is also an enduring example of an intergenerational equity problem. Many of the choices made today will lay the foundation upon which subsequent generations will build. This horizon does not mesh easily with the more limited time constraints that politicians must confront. In other words, 'it's hard to get people to make sacrifices today (i.e., in the form of higher energy prices, less comfortable houses and offices, more expensive travel, etc.) for the sake of people who haven't even been conceived yet.'[464] These trade-offs are also present in the regulatory environment, where greater clarity will reduce ambiguity but, at the same time, reduce freedom of action.

Secondly, many of the cyber-related policy problems that governments are dealing with are neither new nor novel. The difference is not in kind so much as in degree. Cyberspace is less amenable to state control than any other domain. A diverse marketplace is beneficial for competition and innovation but is also harder to control from the perspective of the state. Regulation is done at the risk of driving profitable companies abroad, making compliance and risk management particularly important, yet delicate, topics.

---

464 Stephen M. Walt, 'Who is full of hot air on climate change?,' *Foreign Policy*, 23 July 2012.

Thirdly, national cyber policy is at best immature – where it exists at all – and its development tends to be outpaced by societal exploitation of the domain. Mistakes will be made and accidents and misunderstandings will happen, yet the benefits of global interconnection will continue to outweigh the obstacles. Numerous cyber security concerns will look very different to the next generation, when the number of global users has doubled and the number of connected devices has increased by an order of magnitude. Policy-makers should resist the tendency to overestimate the short-term impact of new technologies, while underestimating their long-term impact.[465]

## 5.2. NATURE OF STATE COMMITMENTS

States make international commitments towards other states, organisations and private entities. This is usually accomplished through the creation of, or accession to, a treaty, but commitments may be made in a variety of ways, and can also create expectations among citizens and other individuals who are affected. It is difficult to categorise state commitments as either legal or political, since they usually contain elements of both.

Commitments may appear to be legal or political, voluntary or mandatory, but they usually have effects that extend outside the originating area. It may be argued that all commitments made by a state are inherently political, even when the content is of a legal character. The political context in which they are entered into can make it difficult to label their acceptance as mandatory, compulsory or optional, at least when these terms are viewed from a legal perspective. However, these labels are of use when discussing the extent to which states have the freedom to interpret and implement the content of a treaty or express an opinion regarding its fulfilment and implementation.[466]

The number of potential new obligations related to the cyber arena is increasing and the nature of cyberspace brings with it increasing demands for international cooperation. This, in turn, may require long-term obligations to be re-evaluated, in order to determine what actions are needed to fulfil respective obligations in a cyber context. There are also more recent commitments that have developed as a

---

465 John Naughton, 'Thanks, Gutenberg – but we're too pressed for time to read,' *The Guardian*, 27 January 2008.

466 See United Nations, *Vienna Convention on the Law of Treaties* (Vienna: United Nations, 1969). Art. 31. The term 'treaty' is used in the generic sense as defined in the Vienna Convention on the Law of Treaties. That is, an international agreement 'governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation' (ibid., art. 2, para. 1(a).).

result of technical advances and the new possibilities cyberspace has brought to society.

### 5.2.1. Legal Commitments

There are numerous international law obligations that have relevance for the area of cyber security, stemming either from treaty law or customary law. States are free to decide which treaties they want to be part of, yet legal commitments which originate from an international treaty are mandatory once a state has signed up to them.[467] However, there are parts of international law that are not optional in two different senses: international law that has reached the status of *ius cogens*,[468] and law that has become customary.[469] There is a difference between them, however, since states are free to agree on and contract customary law aside between each other, which is impossible with law that has the status of *ius cogens*. In addition, it may be noted that some international law treaties are largely unavoidable, either for political reasons or due to inherent treaty functions upon which states are dependent, such as the UN Charter.

Explicit regulation of a specific subject is useful since it provides clear legal advice which, in turn, provides for some predictability of state action. The trade-off with regulations – especially if they concern a specific area – is that they restrict the freedom of behaviour of the state. In addition, as cyberspace is characterised by continuous technical development, the risk of a law, treaty or regulation quickly being outdated is overwhelming. However, in general, trade-offs can be managed, at least to some extent. For example, legal constraints due to regulation of the cyber area can be handled by increased cooperation between actors with different mandates or by designing relevant organisations to enable flexibility of action, thereby achieving the goals and interests of a state and, at the same time, enjoying the benefits of an appropriate legislation. To ensure the attention and implementation of such goals among numerous stakeholders, this needs to be communicated, for example, in a national strategy.

Determining its legal commitments in a cyber context requires a state to take into account (a) the existing explicit commitments made by that state, (b) the obligations that exist due to *ius cogens* and customary law, and (c) the political will

---

467 Ibid., art. 2, para. 1(b).

468 *Ius cogens* is a fundamental part of international law which is binding for all states irrespectively of their explicit consent to it. It cannot be amended or derogated away from it in any way.

469 Customary law is formed by the coherent actions taken by several states for a period of time, treated as a legal requirement. The Statute of the International Court of Justice (ICJ) defines customary international law as 'evidence of a general practice accepted as law' (United Nations, *The Statute of the International Court of Justice* (San Francisco, CA: United Nations, 1945). Art. 38, para. 1(b)).

and ambitions of that state in the digital age. In many cases, treaties constitute the foundation of political commitments for states, and they are then complemented and fulfilled by state actions. Signing a treaty is in itself a political action, showing an explicit standpoint to its content. Political commitments in cyberspace could be demonstrated by adherence to certain standards or through different forms of cooperation. Signing up to a commitment can also bring benefits, from practical actions to demonstrations of intent meant to influence specific stakeholders.

## Charter of the United Nations (1945)

Almost all existing states are members of the UN and thereby obliged to comply with the provisions of the 1945 Charter of the United Nations.[470] The Charter is a multilateral treaty with a dual function; containing (a) rules on how the work of the organisation shall be carried out and (b) rules on the behaviour of states. The Charter contains a supremacy clause that makes it the highest authority of international law. This clause states that the UN Charter shall prevail in the event of a conflict between the (a) obligations of the members of the United Nations under the present Charter and (b) their obligations under any other international agreement.[471] For example, the North Atlantic Treaty refers to the provisions of the UN Charter, clearly indicating its superior status.[472] However, the precise scope and content of the UN Charter is the subject of constant interpretation by states.

The features of the cyber arena pose demands for special interpretation of the Charter, particularly regarding the principles set out in Article 2 on territoriality, equal sovereignty between states and non-intervention in domestic affairs where the features and possibilities offered by cyberspace challenges this part of international law.[473] Another part of the UN Charter which affects national cyber security strategies is Articles 39-42 and 51 on the peaceful settlement of disputes and the prohibition of the use of force. Scholars and practitioners have extensively discussed the applicability and use of these Articles in a cyber context, although the discussions cannot be described exhaustively in this section. In addition, to date there are no formal cases specifically regarding cyber incidents which have been brought up before UN institutions, such as the Security Council. Therefore, states need to consider and seek guidance within their individual existing approaches to this part of international law and evaluate what possibilities, as well as constraints,

---

470 United Nations, *Charter of the United Nations* (San Francisco, CA: United Nations, 1945).

471 Ibid., art. 103.

472 See: United States et al., *North Atlantic Treaty* (Washington, DC: NATO, 1949). Preamble, art. 1, 5, 7, and 12.

473 United Nations, *Charter of the United Nations*: art. 2, 39-42, and 51.

the UN Charter offers when drafting their NCS strategies and how they want to deal with them.[474]

Another concern with regard to the application of the UN Charter is the difficulty of determining and categorising cyber incidents. For practical reasons, it is important that this is done at an early stage of a dispute, in order to be able to address the problem correctly and activate the right players. In short, the inter-connectivity and global character of cyberspace challenges those who use and interpret UN Charter Articles, not least as the digital interdependency between states is increasing. State interests are global and threats are now stemming not just from states, but also from individuals who can leverage cyberspace to reach around the globe. The Charter is without doubt applicable to these new dynamics. The content and design of a state's NCS strategy will have to reflect its contemporary opinion on these issues, while remaining flexible enough to evolve as understanding (regarding UN Charter Articles) continues to grow.

## International Court of Justice (1945)

The Statute of the International Court of Justice (ICJ) is annexed to the UN Charter and all members of the UN are *ipso facto* parties to the Statute.[475] The ICJ's role 'is to settle, in accordance with international law, legal disputes submitted to it by states and to give advisory opinions on legal questions referred to it by authorised United Nations organs and specialised agencies.'[476]

In contentious cases only states are eligible to appear, since the court has no jurisdiction to deal with applications from individuals, non-governmental organisations, corporations or any other private entity. The states concerned in these cases must consent to and accept the Court's jurisdiction, which is a fundamental principle governing the settlement of international disputes. It is worth noting that a significant number of European nations, as well as Canada, only accept compulsory ICJ jurisdiction with reservations, and that the USA has withdrawn its acceptance of compulsory ICJ jurisdiction. In addition, and unlike Europe and Canada, the US is not a participant in the International Criminal Court.

No cases specifically on cyber incidents have been brought before the court, but there are earlier cases with content which has relevance in discussions on cyber

474 One example of this is the Dutch Advisory Council of International Affairs (a civil-society staffed governmental advisory body) report on 'cyber warfare' (See AIV/CAVV, *Cyber Warfare*.).

475 United Nations, *Charter of the United Nations*: art. 93.

476 International Court of Justice, 'The Court,' http://www.icj-cij.org/court/index.php?p1=1.

law. The most important is the *Nicaragua* case,[477] which provides guidance on use of force. In its *Nuclear Advisory Opinion*, the ICJ states that all established principles and rules of International Humanitarian Law apply to all forms of warfare.[478] This clearly also includes the use of cyber means. The court has also provided guidance on the issue of state responsibility in regard to actions of non-state actors in *U.S. v. Iran*[479] (*Hostages)* (1980) and *Congo v. Belgium* (2002).[480] These cases are of importance in a cyber context with regard to the problem of attributing malicious cyber actions to a state.

## International Law Commission (1945)

The International Law Commission (ILC) is a committee of the UN General Assembly that contributes to international law through its mandate, which is to foresee the development of international law.[481] The ILC produces Draft Articles that codify customary law as it should be, according to the opinion of the ILC. As with the ICJ, the ILC has not produced anything specifically regarding cyber but previous work of relevance, especially when drafting a NCS strategy, is its Draft Articles on State Responsibility for Wrongful Acts.[482] These Articles govern when and how states are held responsible for breaches of an international obligation. In this way, they are secondary rules that address basic responsibilities in case of breach of primary rules, for example, a treaty. They also establish under what circumstances an act of an official as well as an individual, may be attributed to a state.

---

477 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, ICJ Reports 1986, 70.

478 The ICJ stated that 'the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict applies to all forms of warfare, and to all kinds of weapons, those of the past, present and the future' (See: *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, ICJ Reports 1996, ICJ 226, para. 86.).

479 *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, ICJ Reports 1981, 64.

480 *Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium)*, ICJ Reports 2002, 3.

481 International Law Commission, United Nations, https://www.un.org/law/ilc.

482 See: *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Report of the International Law Commission. Fifty-third session 2001, Supplement No. 10 (A/56/10). Rather than set forth any particular obligations, the rules determine, in general, when an obligation has been breached and the legal consequences of that violation. In this way they are 'secondary' to the rules regarding the obligation in question, and their general wording also gives room for more specific agreements and regulations. To apply, the international wrongful act must be attributable to a state, and constitute an obligation of that state. This makes it necessary to prove a causal connection between the injury and an official act or omission attributable to the state alleged to be in breach of its obligations. This has become an increasingly significant contemporary issue, as non-state actors play a great role in the cyber area.

## International Telecommunications Union (1865)

The International Telecommunications Union (ITU) is the UN agency for information and communications technology, and is a provider of international telecommunications law. Its work is based upon the ITU Constitution and the ITU Convention.[483] The Constitution contains general provisions regarding obligations and rights for states in regard of telecommunications. Examples of important provisions are found in Section 6 which states that best practices are to be applied regarding the maintenance of telecommunication lines, and that states are obliged to protect and maintain the means for telecommunication.[484] These provisions also apply to the telecommunications means of the internet and since they put specific obligations on states with regard to security and stability of telecommunications, they need to be taken into consideration in a cyber security strategy.

Other legal regulations regarding international telecommunications and wireless internet connections include treaty law on satellite activities made by major satellite companies (which are themselves former intergovernmental organisations). These treaties contain provisions that put restraints on cyber operations, for example forbidding interference with other users, services and equipment.[485]

## UN Group of Governmental Experts on Information Security

To date, there have been a total of five UN groups of experts on cyber-related issues, two of which can be classified as being 'economic' and fell within the remit of the UN Third Committee, and three of which can be classified as 'political-military' and fall within the UN First Committee. It is only the latter that has the official title of UN Group of Government Experts (GGE), although both tracks have run somewhat in parallel to each other.[486] The first GGE in 2004 was created by the General Assembly's First Committee with the second one publishing its report in 2010.[487] In 2004, ECOSOC set up an intergovernmental expert group on identity-related

---

483 See: Additional Plenipotentiary Conference, *Constitution and Convention of the International Telecommunication Union* (Geneva: ITU, 1992). Also see: Additional Plenipotentiary Conference, *Instruments Amending the Constitution and Convention of the International Telecommunication Union (Geneva, 1992), Decisions, Resolutions and Recommendations* (Geneva: ITU, 1994).

484 Plenipotentiary Conference, *Constitution of the International Telecommunication Union (Geneva, 1992) as amended by subsequent plenipotentiary conferences*(Geneva: ITU, 2006). Chapt. VI, art. 38.

485 See: INTELSAT General Corporation, 'Terms of Use,' http://www.intelsatgeneral.com/terms. Also see: Inmarsat, 'Legal notices. Terms and Conditions of Use,'http://www.inmarsat.com/Terms_and_conditions.aspx.

486 See Tim Maurer, Cyber Norm Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-Security, (Cambridge, MA: Belfer Center for Science and International Affairs, 2011), http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

487 Ibid.

crime which has evolved into the core group of experts.[488] The ITU set up a high-level expert group that developed the Global Cybersecurity Agenda in 2007 and the United Nations Congress on Crime Prevention and Criminal Justice established an open-ended intergovernmental expert group on cyber crime in 2010.[489] Due to the complexity of the issues involved, the First Committee Group was unable to reach a consensus on a final report, but the second (2009-2010) produced a report on law applicable in the context of cyber security and confidence building measures in cyberspace.[490] Both groups have examined and described existing and potential threats against information security as well as what challenges this will bring to society. The last report stresses the need for shared perspectives among states, and practical cooperation by a broad range of activities, such as sharing best practice, exchange of information and capacity building. The reports are of high value for states, providing guidance on threats as well as measures that need to be taken towards achieving increased information security, stability and resilience in cyberspace.

A third GGE was established in 2010 by a UNGA resolution[491] to follow up the work of the previous groups and to continue to study the 'existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of states and confidence building measures with regard to information space'. This group will initiate its work in 2012 and report in September 2013.

### 5.2.2. Cyber-Enabled Terrorism

It is reasonable to presume that cyberspace could be used as a vector for initiating physical attacks to further the aims of a terrorist: terrorist groups also use cyberspace to recruit, spread propaganda and organise their activities. Terrorism is prohibited in both international and national law (since national legislation needs to be complemented by international measures due to the character terrorist acts

---

488 Ibid.

489 Ibid.

490 See: Group of Governmental Experts, Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201), (New York: United Nations, 2011), http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf. This report was followed up by another report on the same topic where the Member States had the opportunity to express their opinions on the content of the first report, see: UNGA, *Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/66/152/Add.1)* (New York: United Nations, 2011). More information on the evolution of the First Committee's position on cyber security can be found here: Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-Security.*

491 UNGA, *Developments in the field of information and telecommunications in the context of international security (A/RES/66/24)* (New York: United Nations, 2011).

may take). States and organisations which support terrorist actions may become responsible for the acts of that subject on the same legal grounds as described above on the judgements of the ICJ.[492] Cyber terrorism is not specifically proscribed in any international convention, which is of special importance due to the fact that international law on terrorism is scattered, and the means used (cyber technique, kinetic energy, etc.), have an effect on the applicable law.[493]

There is no overarching general convention on terrorism[494] but, in 2006, the UN General Assembly adopted a resolution called the Global Counter-Terrorism Strategy.[495] The strategy consists of a resolution and an annexed Plan of Action, and underscores the importance of existing international counter-terrorism instruments by pledging Member States to becoming parties to them and implementing their provisions. The strategy provides Member States with a common strategic approach to fight terrorism, not only sending a clear message that terrorism is unacceptable in all its forms, but also resolving to take practical steps individually and collectively to prevent and combat it. Acts of cyber-enabled terrorism are encompassed by this strategy, however, since it merely encourages states to take necessary measures, it needs to be read together with, and is complemented by, regulations that deal the inherent specific features of cyber-enabled terrorism and cyber crime. In addition, UN Member States are currently negotiating a Draft Comprehensive Convention on International Terrorism, which will complement the already existing conventions on the topic.

---

492 It is an extensive discussion regarding circumstances when a state should be responsible for such acts, which cannot be dealt with in detail in this manual. For further guidance on this matter, see: *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. Also see: *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*.

493 Examples (not exhaustive) of very specific regulations on terrorism are the ICAO, *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation ('Montreal Convention') (974 UNTS 177)* (Montreal: International Conference on Air Law, 1971). Also see UNGA, *International Convention for the Suppression of Acts of Nuclear Terrorism (A/59/766)* (New York: United Nations, 2005). For a complete list, see: http://www.un.org/terrorism/instruments.shtml.

494 Since 1963, the international community has elaborated 14 conventions (of which 12 are in force), and four amendments to prevent terrorist acts. Those conventions are developed under the auspices of the UN and they address specific terrorist acts, like bombings, or specific environments, like the maritime safety.

495 UNGA, *The United Nations Global Counter-Terrorism Strategy (A/RES/60/288)* (New York: United Nations, 2006).

In 2002, all EU Member States agreed on a definition of terrorism to be used in national legislation,[496] and the Council of Europe subsequently adopted the Convention on the Prevention of Terrorism (2005).[497] A defining feature of the Convention is Article 5, which contains a definition of a 'Public Provocation to Commit a Terrorist Offence', the first attempt by international law to define incitement to terrorism. It is controversial due to the inclusion of 'indirect' incitement. The limits of this concept are not defined; however Article 12 requires parties to implement the offence in a way that is compatible with the right to freedom of expression as recognised in international law. States face a challenging task balancing the prevention of terrorism (including cyber-enabled terror) with the requirements of the Convention and relevant human rights principles.

### 5.2.3. Cyber Espionage

One prominent area of international law where states clearly prefer not to have a specific international regulation is espionage or, in this context, cyber espionage. There is a range of probable reasons why states have chosen to keep this area legally unregulated but most tend to revolve around the benefits that this ambiguity provides. It could be argued that acts of espionage are banned by the principles of the UN Charter Article 2 on sovereignty and non-intervention in internal affairs, but there are very few cases where a state has taken action in accordance with these regulations.[498]

National legal obligations and the limits of state action are often regulated by the constitution of the state. Legal obligations in international law are, to a large extent, subject to the opinions of states, since they have flexibility to choose the scope and content of their obligations. However, once adhered to, it is difficult for a state to withdraw from commitments, although there may exist a margin of appreciation on the degree of flexibility states are permitted during the fulfilment of their obligations. This is determined by the status and design of the legal instrument in question. States commit themselves to obligations in expectation of certain benefits. But there is usually a trade-off involved in this process, for example, taking

---

496 *Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)*, Official Journal of the European Union, L 164. This has been changed by another decision in 2008 (*Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*, Official Journal of the European Union, L 330.), although the definition of a terrorist crime was not changed. A terrorist crime is defined as any of the offences defined under the 12 existing international conventions on terrorism presently in force, complemented by additional provisions.

497 See http://conventions.coe.int/Treaty/en/Treaties/html/196.htm.

498 For one example, see: the '*Rainbow Warrior Case*' arbitrated by a tribunal chaired by then Secretary-General of the UN in 1986, see: *Rainbow Warrior Case (New Zealand v. France). Ruling of the UN Secretary-General of 6 July 1986*, 74 ILR 241.

a strong stand for human rights principles is a form of self-imposed restriction, and may make it more difficult or expensive for a state to fulfil other tasks. Regulations also restrict state behaviour in the sense that, if a state that commits itself to a certain rule, it is obliged to adhere to it. Therefore choosing not to regulate can also be an advantage, in order to maintain a state's freedom of action. Contrary to international law, espionage is commonly regulated in national criminal law as a crime if committed by an individual. This is an effect of the need for states to provide themselves with legal instruments to restrict as well as prohibit espionage on its territory against its interests. However, the criminalisation of terrorism and espionage in the domestic legal system does not have any effect outside the jurisdiction of the state.

Espionage in cyberspace can be conducted by Computer Network Exploitation (CNE),[499] which is an action to explore and investigate the technical structure, design and content of a certain area of cyberspace. However, unless conducted in accordance with the national criminal law requirements – which generally demand that espionage provides a state with information which otherwise would be impossible to retrieve – CNE is a mere intrusion and possibly a crime. This is a complicating factor for international law.

The possibilities that digitisation of society offers for CNE are vast – not just for states, but for organisations, commercial entities and individuals. This can come from any part of the world, for any reason, against a broad range of targets from military weapon systems to the civilian telecom industry.

A comparison between cyber espionage which has no explicit regulation in international law, and cyber-enabled terrorism, gives us a picture of states trying to handle two types of threats in very different ways: the first by avoiding legal commitments, and the latter by numerous and detailed legislation.

### 5.2.4. Cyber Criminality

All legal obligations require implementation but the strictness and detail of the demands posed on states differs. One area that benefits from detailed implementation is the countering of cyber criminality, or cyber crime.[500] Due to the global penetration of information and communications technology (ICT) in all aspects of society, as well as the interconnected nature of the internet, cyber criminal acts are easy to commit abroad. This makes it fundamental that states cooperate

---

499 The implications of the CNE definitions within the context of 'cyber attack' are discussed in Section 1 and Section 3.

500 See Section 1.2 for a discussion on cyber crime.

and support each other on these matters, which brings with it responsibilities, as well as legal obligations. Combating cyber criminality has become an activity of interest for all actors concerned with information security. Due to this, the topic benefits should be addressed from a governmental level in order to ensure coherent and coordinated efforts.

Cyber crime can be conceptualised either as a 'new' or an 'ordinary' type of crime[501] committed in, or by, the use of cyber means and infrastructure. For example, unauthorised access (intrusion) into closed networks, or the construction and use of botnets, are crimes that have evolved due to technical developments. They stand side by side with 'ordinary' crimes such as theft, fraud, sabotage and threatening behaviour, all of which are also now possible to commit in cyberspace. Due to this, two 'ordinary' types of crime: terrorism and espionage, are dealt with separately in this section because of their special features and effect on the digital, interconnected world.

The International Criminal Police Organisation (INTERPOL) has recognised the evolving problem of cyber crime and has launched a programme in response. It consists of eight main points and contains both training and operative measures.[502] INTERPOL has concluded cooperation agreements with international organisations such as the UN and the EU in order to fight international criminality. This has enabled cooperation with the European Police Office (EUROPOL) which was founded in 1992[503] and which became an official organ of the EU in 2010,[504] in response to the European Commission's communication '*Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*'.[505] EUROPOL is Europe's specialist centre on law enforcement and provides analytical expertise and operational support on cyber criminality. The recently established European Cybercrime Centre (housed in EUROPOL) has a slightly different aim; to pool expertise and information and collaborate with key EU stakeholders, non-EU countries, international organisations, internet governance bodies and service providers, internet security companies, the financial sector, academia, civil society organisations and CERTs as to become the focal point in the EU's fight against

---

501 See, for instance, European Commission, *Towards a general policy on the fight against cyber crime (COM(2007) 267 final)* (Brussels: European Commission, 2007).

502 For more information, see: INTERPOL, 'Cybercrime,' http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

503 A European Police Office for the cooperation between Member States was mentioned in the European Union, *Treaty on European Union ('Treaty of Maastricht')* (Brussels: Official Journal C 191, 1992). Art. K.1(9).

504 *Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA)*, Official Journal of the European Union, L 121.

505 European Commission, *Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM(2012) 140 final)* (Brussels: European Commission, 2012).

cyber crime.[506] It supports Member States and the EU in building operational and analytical capacity for investigations and cooperation with international partners including non-EU countries.

In 2002, the EU presented a proposal for a Framework Decision on Attacks against Information Systems, which takes note of the Convention on Cybercrime, but concentrates on the harmonisation of substantive criminal law provisions that are designed to protect infrastructure elements.[507, 508] The Framework Decision has been reworked and a revised version is expected to be adopted in the fall of 2012. This version substantially strengthens both the minimum penalties involved while, at the same time, seeks to strengthen the legal environment to encourage the adoption of better information security principles by legal persons.

### 5.2.5. Convention on Cybercrime

Several initiatives have been taken to increase international cooperation and fight cyber crime.[509] One of the most important legal instruments in the fight against cyber crime is the Council of Europe Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, described below. It is the only binding international treaty on the subject that has been adopted to date. The Convention is open to signature by non-European states, and there are currently 47 signatories, of which 37 have ratified the Convention. It provides guidelines, including legislative direction, for all governments wishing to protect against cyber crime.[510] Its objective is to pursue a common criminal policy, particularly through adopting appropriate legislation and fostering a fast and effective regime of international cooperation. This is done through developing legislation against cyber crime; harmonising domestic criminal laws (such as substantive law elements of offences); improving investigative technique; providing

---

506 The centre will be operational by 1 January 2013, see: Europol, 'European Cybercrime Centre to be Established at Europol,' *Media Corner*, 28 March 2012.

507 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, Official Journal, L 201.

508 *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*, Official Journal of the European Union, L 69.

509 The European Commission on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, the EU Forum on Cybercrime, the OECD Security Guidelines and the G8 Committee on High-Tech crime, the UN General Assembly Resolution on Combating the Criminal Misuse of Information Technology (2000, 2002).

510 As early as 1997, the G8 released an action plan and principles to combat cyber crime and protect data and systems from unauthorised impairment. Later, the G8 called for standardisation on laws on cyber crime, cross-border communication and enhanced cooperation on extradition cases of suspected cyber criminals. This was made at the same time the Council of Europe launched the Convention on Cybercrime, which met the essential demands of the G8.

for domestic criminal procedural law powers, and prosecution of such offences as well as other offences committed by means of a computer system (or related evidence which is in electronic form).

The Convention provides legal solutions aiming to tackle the consequences of criminality taking advantages of the global nature and anonymity of cyberspace. It provides guidelines and legislative direction for all states wishing to protect themselves against cyber crime in cooperation with other states. The Convention creates stipulations for the most important actions which need to be taken to combat cyber criminality but, at the same time, gives some leeway which facilitates implementation. For example, the content of the Convention does not have to be copied into the domestic legislation of the states (for ratification, states need to have laws which provide an equivalent framework to the content of the Convention); some Articles allow states to add qualifying circumstances, and the offences listed in Chapter II of the Convention are considered a minimum-standard model which means states are free to legislate more extensively on these matters.

The aim of the Convention is to pursue a common criminal policy, particularly through adopting appropriate legislation and fostering a fast and effective regime of international cooperation.[511] This is done through (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber crime, (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by the means of a computer system or evidence in relation to which is in electronic form, and (3) setting up a fast and effective regime of international cooperation.[512] The content is divided into four chapters (use of terms, measures on substantial and procedural law, international cooperation, and final clauses), but the commentary here is concentrated on Chapters II and III.

## Chapter II

Chapter II contains three sections: *substantive criminal law* (Articles 2-13), *procedural law* (14-21) and *jurisdiction* (22). The first section lists relevant offences, thereby aiming to create a common minimum standard which makes it difficult for perpetrators attempting to perform their illegal activities in states with lower standards or even lack of criminalisation of such activity. Another positive effect of coherent legislation is that extradition between states is facilitated when the offence is criminalised in both of them. The offences which the Convention lists

511 Council of Europe, Council of Europe Explanatory Report to the Convention on Cybercrime (ETS No. 185), (Strasbourg: Council of Europe, 2001), http://conventions.coe.int/Treaty/EN/Reports/html/185.htm. Para. 16.

512 Ibid.

cover crimes which are computer-related, such as illegal access (unauthorised access into computer systems and data); illegal interception (monitoring or surveying communication without right); system interference (seriously sabotaging the function of computers and data), as well as ordinary crimes committed by the means of computers such as computer-related forgery and fraud. Finally, the last Article of Section 1 is another example of the Convention not over-regulating the matter: instead of requiring specific sanctions and measures for each crime, the Article requires states to 'adopt such legislative and other measures as may be necessary to ensure that the criminal offences [...] are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.'[513]

The second section contains provisions for procedural law issues which concern the obtaining and collection of data for criminal investigations and proceedings. It applies to the offences established in the first section but also to any offence committed by the use of computers as well as electronic evidence. The first Articles (14-15) contain safeguards provisions which require the states to ensure that the obligation to introduce the procedural law provisions do not interfere with human rights or the principle of proportionality. The following Articles (16-17) apply to data which is stored, for example, at telecom companies and Internet Service Providers. The Convention requires that competent authorities have the right to obtain such computer and traffic data for criminal investigations and proceedings. This is very important legislation for states to have in place since, if the data is impossible to retrieve, investigations and the possibilities of providing support and cooperation with other actors will be seriously hampered. Article 19 contains procedural rules on search and seizure of stored computer data. This type of rule exists in domestic legislation with regard to tangible objects and the Convention provides guidance on how to modernise such laws in order to ensure effectiveness for electronic data. However, due to the interconnectivity of computer systems, there is always a risk that data is stored outside of a jurisdiction. Therefore, the need for trans-border actions requires international cooperation, which is addressed in Chapter III. Collection of real-time traffic and content data is addressed in Article 20 and 21. Often these rules, like search and seizure, already exist in domestic legislations with regard to telecommunications, and the Convention provides guidance on how to apply it to computer data.

The third section contains one provision on jurisdiction. The Article is based on the international law principle on territoriality and contains criteria under which states have to establish jurisdiction.[514]

---

513 Council of Europe, *Convention on Cybercrime (ETS No. 185)*: art. 13.

514 Ibid., para. 232-9.

### Chapter III

Chapter III describes international cooperation and provides an important addition to the provisions in Chapter II. As mentioned earlier, the interconnectivity and global features of cyberspace, the inherent character of volatility with regard to computer data, and the possibilities of deception and anonymity create conditions which require states to be willing and able to work together by providing mutual support and cooperation in order to fight cyber criminality. Chapter II describes *what* needs to be in place and, to gain effect, Chapter III describes *how* to achieve this, for example, by providing rules on mutual assistance and extradition.

The Chapter is introduced by Article 23 which contains general principles on international cooperation: cooperation is to be provided to the widest extent possible, on all criminal offences within the scope of this Convention and, in accordance with the provisions of the Convention, relevant international agreements and domestic laws.[515] The following Articles are detailed rules which form a coherent and effective framework which gives directions on what domestic laws need to be in place, as well as information on cooperation and the like. Article 24 deals specially with extradition, an area where international and bilateral agreements often are in place, and the provisions cover both situations where there are rules already in place between the states, as well as when such legal basis does not exist. Articles 25-34 contain substantial stipulations on mutual assistance and cooperation on criminality, collection of electronic evidence and more and, in order to further enhance and secure the operational effects of the Convention, Article 35 requires states to arrange for a point of contact available 24/7. The aim is to ensure rapid response to requests for assistance either by facilitation, direct measures or coordination with relevant components. This means that the 24/7 units need to be provided with appropriate skills and a mandate which ensures a quick and effective response. The data for investigations is to be provided via the Mutual Legal Assistance Treaty (MLAT) which regulates these exchanges. Chapter III also holds Article 32 (b), which effectively allows law enforcement to access data held abroad. This is the most significant challenge to Russia, which has used Article 32 (b) as a reason to reject the entire Convention.

## 5.2.6. Human Rights

The most important parts of human rights legislation in a cyber context are the rights to freedom of expression and opinion, and the right to privacy. The internet has become an indispensable tool for the exercise of these rights, which makes access to the internet an important priority for states that are interested in

[515] Ibid., para. 243-4. Note that Article 24, and 33-34 permit a different scope of application.

supporting these rights. In some states, internet *access* as such is seen as a human right.[516] However, this standpoint has been criticised by those who argue that the internet is merely a tool for exercising pre-existing rights. They also emphasise the development of national cyber policies to make internet available and accessible for all individuals, free from restrictions on its content. Mere access means little by itself, if content is subject to censorship and restrictions.

Freedom of expression may bring with it inconvenience for states, since it may be used as a tool for raising political awareness, criticising and holding governments responsible for their actions. A drawback to freedom of expression is that, to a certain extent, it may permit the flow of information of a criminal character. However, security measures – such as blocking, filtering, banning, enforcing real-name policies, censorship, speech criminalisation and surveillance – must be carefully considered as they may pose a threat to human rights. State-sanctioned police and intelligence powers are necessary in order to fulfil societal obligations and human rights law does not prohibit them as long as they are designed and used with care and consideration.

The UN Universal Declaration on Human Rights is a UN General Assembly declaration codifying human rights.[517] The declaration defines the fundamental rights of individuals, and exhorts all governments to protect these rights. Provisions of interest in a cyber context are Article 12 on the protection from arbitrary interference by authorities[518] and Article 19 which contains the right to freedom of expression.[519] However, all Articles are subject to a general exception which give states right to limit rights and freedoms of individuals for purposes vital for the function of the society.[520]

The UN International Covenant on Civil and Political Rights (ICCPR) is an international instrument for human rights. It is a multilateral treaty adopted by

---

516 In Estonia, Finland, France, Greece and Spain, internet access is a legal right.

517 Declarations of the UN General Assembly are not legally binding for states according to the UN Charter Articles 10-17. Although parts of the declaration are considered to reflect customary law, there is no consensus on the specific parts this reflection may encompass.

518 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

519 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.'

520 Article 29 states: 'In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.'

the General Assembly in 1966,[521] and is the first universal human rights treaty.[522] It differs from the universal declaration mentioned above, since Part II of the covenant contains a positive obligation on states to undertake necessary measures to provide effective remedies for individuals who think their rights according to the covenant have been violated. Enforcement of the covenant is to some extent undermined by the reservations made by states which render ineffective the covenant rights which otherwise would require changes in national law to ensure compliance with covenant obligations.[523]

The European Convention on Human Rights (ECHR) is a European initiative regarding human rights that established the supranational European Court of Human Rights.[524] Parties to the Convention include all 47 Member States of the Council of Europe. Its provisions are written in general terms, which leads to a need for clarification in certain circumstances (and which is met by interpretative court decisions). Individuals have a right to bring their claims to the court and Member States – in cases where the court decides there is a violation – are bound to comply with and execute the court's decision, which gives the Convention a strong legal impact upon states.

Provisions of interest[525] in the cyber context are Articles 8 and 10. Article 8 protects individuals from unlawful searches and arbitrary interferences by public authorities, but the scope of the provision is even broader due to the protection of 'private and family life'.[526] In a cyber context, this indicates that the provision is applicable not only to personal data and other information owned and stored by an individual, or

---

521 The covenant came into force in March 23, 1976.

522 There are also numerous regional human rights treaties worth to be mentioned; the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), the American Convention on Human Rights (ACHR), the African Charter of Human and Peoples' Rights, and the Cairo Declaration on Human Rights in Islam.

523 Jamal Greene, 'Hate Speech and the Demos,' in *The Content and Context of Hate Speech: Rethinking Regulation and Responses*, ed. Michael Herz and Péter Molnár (Cambridge et al.: Cambridge University Press, 2012).

524 European Court of Human Rights, www.echr.coe.int.

525 A comprehensive research report on case law regarding internet-related matters has been made by the research division of the court; 'Internet: case-law of the European Court of Human Rights' and the following discussion is based on the findings of the division. For the full report, see: Research Division, Internet: case-law of the European Court of Human Rights, (Strasbourg: European Court of Human Rights, 2011), http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_internet_Freedom_Expression_EN.pdf.

526 Article 8: '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

to e-mail exchanges, but also to ICT-based systems and networks including internet traffic. There are also positive obligations for the authorities inherent in the respect for private or family life, for example, a duty to ensure an effective deterrent against grave acts to a person's personal life. The compilation, storage, use and disclosure of personal data by authorities constitutes interference with the rights as set out in Article 8, however, such data may be collected and stored in the interests of national security as long as there are adequate and effective legal guarantees against abuse.

Article 10 on the freedom of expression – of which the internet has become an important tool – deals with a basic right in a democratic society.[527] The court has taken a position in case law that offers little room for restrictions on this right by state authorities. The right to 'receive and impart information [...] regardless of frontiers' also prohibits states from actions aiming to censor internet content by blocking, filtering or otherwise restricting access to information which others are willing to impart.[528]

States are obliged, not only to ensure their citizens are able to exercise their legal rights, but also to ensure their protection and security. These duties are sometimes in conflict and states need to find a balance in order to fulfil these interests. The case law of the court provides valuable guidance on these matters, ensuring the protection of individual rights and freedoms and, at the same time, recognising the needs of authorities to ensure the function of the democratic society.

### 5.2.7. International Humanitarian Law

The purpose of International Humanitarian Law (IHL) is to limit the hardship and suffering of the civilian population and combatants during conflict, by providing a minimum standard of protection. The main treaties are the Geneva Conventions and its Additional Protocols, as well as the Hague Conventions. Significant portions of these treaties are also recognised as customary law and contain rules for warfare such as the principles on proportionality, necessity, distinction and non-discrimination. The use of IHL is of great importance regarding the deployment

---

527 Article 10: '1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent states from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.'

528 Note that Article 10 does not provide a right for individuals to access all official documents of a state. Information may be restricted from public access due to conditions prescribed by law and for reasons necessary in a democratic society.

of cyber effects in conflict situations, due to the inherent nature of civilian and military functions within the same areas. The centre of gravity in cyber conflict situations is, due to the nature of cyberspace, likely to take place amidst the civilian population. Therefore states needs to pay attention to IHL at the government level when assuming and designing its commitment to military operations and military forces need to exercise due care and attention to the interpretation and application of IHL regulations, since this will direct the scope and content of military rules of engagement and national caveats.

As evident from its purposes and scope of regulation, the rules of IHL are applicable in armed conflict situations, declared war and occupation.[529] Internal domestic conflicts complicate the landscape, as IHL only applies if the conflict reaches the threshold of a non-international armed conflict (e.g., 'civil war'). However, the difference between the legal rules regarding these types of conflict has diminished. For example, since 1996, all IHL treaties that have been created are applicable in both types (internal and external) conflict.[530]

IHL instruments do not reference 'peace-keeping forces', but the UN has provided clear directions that peace-keepers need to apply IHL and, as far as applicable, also human rights.[531]

However, problems can still occur when the same force comprises troops from states that are party to IHL treaties and states that are not. One solution provided by the EU is the European Union Guidelines on promoting compliance with international humanitarian law, which provides operational tools for Member States and ensures coherent compliance in all actions taken by the EU within this area.[532] The guidelines encourage Member States to comply with their obligations according to IHL in applicable situations. The guidelines may also be applied on non-state actors if this is in the interest of a Member State. This last provision is of interest in a cyber context, due to the fact that malicious code can be developed and used by individual actors, in addition to problems with a definitive attribution to a perpetrator.

---

529 ICRC, *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention)* (Geneva: ICRC, 1949). Art. 2.

530 See, for example, the Convention on the Prohibition, Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction (1997) (also 'Ottawa Treaty'), or the Convention on Cluster Munitions (2008).

531 UNSG, *Secretary-General's Bulletin: Observance by United Nations Forces of International Humanitarian Law (ST/SGB/1999/13)* (New York: United Nations, 1999).

532 *European Union Guidelines on promoting compliance with international humanitarian law (IHL)*, 2009/C 303/06.

The features and use of malicious cyber activities in non-armed conflict situations, as well as the scope and consequences of cyber criminality, have stimulated discussions among lawyers on the applicability of IHL principles regarding peacetime incidents in cyberspace.[533] The value of these analyses remains primarily academic, as the chances of practical use is limited due to the fact that states are generally reluctant to formally declare themselves in situations of armed conflict due to the range of additional consequences this brings.

Important guidance regarding the applicability of IHL to cyber activities will be found in the Manual on the International Law Applicable to Cyber Warfare (also known as the Tallinn Manual). The manual was written by an international independent group of experts, invited by the NATO Cooperative Cyber Defence Centre of Excellence. It aims to provide interpretations on how IHL applies in cyberspace, as well as to generate and deepen discussions on these topics between lawyers at the international level.[534]

### 5.2.8. Legal Thresholds

Cyber incidents can encompass a wide range of activities. This means there are different definitions, or legal categories, depending on the character of the incident. These categories are separated by thresholds. In essence, a threshold evolves when a legal framework changes due to the shift in the characterisation of an incident. Thresholds are closely linked to the provisions of the UN Charter but also to the problem of attribution. With regard to the UN Charter, only states are subject to its provisions. Therefore, without a positive attribution to a state, the Charter is not applicable. The assumptions are likely to be that the perpetrator is an individual, and the cyber incident at stake will be labelled as cyber crime or cyber terrorism, which calls for the application of criminal law, not the UN Charter.[535]

If cyber incidents (initially) are likely to be regarded as crimes, they will be handled by the police. However, in addition to the overall context, investigations will show the extent and severity of the threat and whether it is to be attributed to an individual (situated domestically or abroad) or a state. Depending on what information can be provided to the legal evaluation, it is to be decided if the incident has reached another threshold, which opens up a different definition and a different legal framework. This situation calls for cooperation. A NCS strategy would benefit

---

533 See also Section 1.4 and Section 3.1.3 for a discussion on cyber attacks.

534 For more information about the manual, see Schmitt (gen. ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

535 The principle on state responsibility is relevant in this context, as well as international law on attribution of responsibility of a State on activity performed by individuals. These topics are further discussed in this on ILC and ICJ.

from addressing the need for fast and efficient cooperation on these matters, in order to prevent from responding incorrectly or too late.

Regarding actions of states, three thresholds will be mentioned:[536] (1) the UN Charter Article 2(4) which contains the prohibition of *use of force* (which is when a state breaches a peacetime rule); (2) the UN Charter Article 39 clarifying when an incident amounts to a *threat or a breach of the peace* or an *act of aggression* (which calls for action from the UN Security Council), and (3) the UN Charter Article 51 which gives a state the right of self-defence in response to an *armed attack*.[537]

Article 2(4) prohibits the threat or use of force between states.[538] The use of force is traditionally regarded as the use of kinetic force which brings with it death or injury to persons, or damage and destruction to objects. Cyber incidents may generate a range of effects, including incidents similar to kinetic attacks. But the means of accomplishing such incidents are generally different. Guidance is provided by the ICJ which states in the *Nicaragua* case that actions of non-kinetic nature can be regarded as a use of force.[539]

Articles 39-42 regulate under what circumstances the UN Security Council can decide that a situation represents a threat, a breach to peace or an act of aggression (Article 39). It is also clarified if action is to be taken by the international community in accordance with Article 41 and 42 to restore international peace and security. The Security Council has chosen to categorise a wide range of situations within Article 39 ('threat or breach to the peace'), including civil war, large numbers of refugees threatening to destabilise a region, or the degradation of democratically elected political leaders. The basis for this decision was not purely legal, but also accounted for global processes as well as political reasons, since Article 39 'opens up' for Articles 41 and 42. What constitutes an 'act of aggression' is defined in the UN General Assembly resolution 'Definition of Aggression'.[540] It is increasingly assumed that cyber incidents of a certain extent and effect can fall within Article 39, especially taking into account the interconnectivity and the global nature of cyberspace.

Article 51 of the Charter gives states a right to self-defence in case of an armed attack. There has been extensive debate on whether a computer network attack

---

536 Cyber criminality is addressed in chapter 5.1.3.

537 For an excellent and comprehensive discussion on these topics, see Michael N. Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited,' *Villanova Law Review* 56(2011), http://www.usnwc.edu/getattachment/f1236094-416b-4e5b-bf58-32e677aed04a/villanova_cyber_ad_bellum.

538 This is also recognised as customary law, see *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Para. 98.

539 Ibid. Note 4 para. 228.

540 UNGA, *Definition of Aggression (A/RES/3314(XXIX)* (New York: United Nations, 1974).

can amount to an armed attack. However, in order to find an answer, one must try to define 'armed attack' in the cyber context. Again, the notion 'armed' is targeted at kinetic force, which brings with it death or injury to persons, and damage and destruction to objects.[541] From an effect-based approach, cyber incidents generating such consequences could fall within Article 51, giving the target state a right to respond by necessary and proportionate means.

## 5.3. INTERPRETATION OF COMMITMENTS

When states decide to adhere to a certain commitment, each party will perceive the content of that commitment differently. The extent of these differences is dependent on the nature and context of the commitment, as well as on the mood and the strength of the respective government. The differing interests of states, and their relative positions of power in cyberspace, will be reflected in their NCS policies. This, in turn, inevitably means that the implementation and the fulfilment of commitments will vary. States can choose what obligations they accept and what obligations they adhere to, and will decide their level of commitment in line with the national need.

If the economic, social and security benefits of an obligation outweigh the costs and constraints, the state can make the decision to adhere to it. However, this judgement will vary from state to state based on the individual interpretations of the content of the obligation. In some cases, these interpretations can be overruled by the European Convention on Human Rights, where the court has the authority to make binding decisions on a state's interpretation and implementation of the Convention.

The implementation of a state's commitment is crucial for the effect it will have. Due to the pervasive character of cyberspace, cyber issues often require a broad perspective. Depending on the complexity and scope of the specific obligation, there might be a need to engage a broad range of government departments.[542] Delivery in a stovepiped manner, or by a single department, risks a narrow or ineffective solution. An example of a commitment requiring the engagement of several departments is the objective of the European Commission's Digital Agenda, which is to 'deliver sustainable economic and social benefits from a digital single market'.[543] To make this type of commitment work, states need to ensure adequate

---

541 Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited'. 588.

542 See Section 4 for a broad discussion on operational cooperation.

543 Directorate General for Internal Policies, Briefing Note: Digital Agenda for Europe – An Overview for the 37th EEA JPC, (Strasbourg: European Parliament, 2011), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/deea/dv/1011_10_/1011_10_en.pdf.

cooperation between agencies as well as measures that facilitate shared tasks and responsibilities.

### 5.3.1. Governance

Governance of the cyber domain – in particular of the internet and its networking protocols – is the remit of a number of organisations which this section will mention, in addition to a myriad of stakeholders which are beyond the scope of this enquiry. Cyberspace is an environment that states operate within and, to a certain extent, can influence but not control. From NATO's perspective the primary, initial challenge is to decide its role in the global cyber ecosystem. And, subsequently, it must divide responsibilities between its command structure and the forces assigned to it. In other words, what tasks does NATO carry out and how much does it rely on Member States?

Recent national policy initiatives have recognised the importance of addressing cyber governance from a variety of perspectives. Commercial incentives drive the vast majority of the market for cyber security goods and services. Government is a non-negligible player in the procurement market for ICT goods and services, and has an interest in promoting secure products (e.g., Trusted Computing Group[544]). The economic aspects of cyber security are also of increasing prominence, as noted in the 2011 UK Cyber Security Strategy – sub-titled 'Protecting and promoting the UK in a digital world'.[545] However, for NATO, which is designed to be a political-military alliance, its interests in cyberspace could be said to coalesce around a number of primary areas or mandates.[546] This includes military activities, counter-crime, intelligence and counter-intelligence, critical infrastructure protection and national crisis management, and diplomacy and internet governance.[547]

The governance of cyberspace is of international concern, given the inherently international nature of cyberspace and its attendant risks and opportunities. National cyber security policies would benefit from adopting a broad perspective and viewing the digital domain from beyond a purely military viewpoint. There are a number of governance-related organisations that are of relevance to security policy-makers. One of the most influential is the Internet Corporation for Assigned Names and Numbers (ICANN), which is a non-profit private organisation based in the US. The importance of ICANN stems from the organisation's work on the coordination of the internet systems of unique identifiers by coordination of IP addresses and the

544 Trusted Computing Group: http://www.trustedcomputinggroup.org.

545 UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.*

546 Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65).* 15-9.

547 These mandates are introduced in Section 1 and described in more detail in Section 4.

Domain Name System (DNS), a hierarchical organisation of namespace that is vital for the functioning of the internet. For most governments, the local registries[548] are even more important, as they manage the internet space for a national top-level domain (such as .fr or .de) and have a direct relevance for NCS. Registries often work through local groupings such as the Regional Internet Registries (RIR), and the RIR responsible for Europe and the Middle East (RIPE) also maintains its own Network Coordination Centre. Other relevant organisations include protocol and standard setting groups which, for the most part, are simply collections of volunteer engineers. A preeminent example is the Internet Engineering Task Force (IETF), a pure volunteer network of engineers which produces technical and good practice documents called RFC (Request for Comments). The IETF is a famously anarchic organisation that, officially, does not even exist (it is a subchapter of the Internet Society). However, there are few technical organisations that have done as much to help build (and fix) the internet, or whose influence has gone as unnoticed for so long. In recent years, however, there has been a clear movement of large private sector companies (including Chinese hardware manufactures) into the IETF – many of the more recent RFCs were probably directly drafted with specific industry backing. Government, in comparison, still plays a very minor role among IETF experts.

Related telecommunications issues are dealt with by the International Telecommunication Union (ITU) which is the UN agency for information and communication technologies. ITU is founded on two documents: the ITU Constitution and the ITU Convention.[549] The ITU has 193 members, as states become parties to the organisation automatically by its affiliation to the UN. However, UN Member States are free to decide what support they want to contribute.[550] The ITU is based on public-private partnership and, in addition to the states, over 700 private-sector entities and academic institutions are members. Its main efforts are to be found within the technical domain regarding three main areas of activity; radio communications (coordination of radio communication services and the international management of the radio-frequency spectrum and satellite orbits), standardisation (fundamental for internet access, communication protocols, voice and video compression, home networking, and other telecom protocols)

---

548 Also known as 'country-code top level domain' (ccTLD) registries.

549 See: Additional Plenipotentiary Conference, *Constitution and Convention of the International Telecommunication Union*. Also see: Additional Plenipotentiary Conference, *Instruments Amending the Constitution and Convention of the International Telecommunication Union (Geneva, 1992), Decisions, Resolutions and Recommendations*.

550 For the position of UN Member States that have signed, but not ratified the ITU Constitution and Convention, see: Plenipotentiary Conference, *Constitution of the International Telecommunication Union (Geneva, 1992) as amended by subsequent plenipotentiary conferences*: chapt. IX, art. 52.

and development (programmes for various purposes such as development of connectivity or enabling telecom expansion in emerging markets).

In addition, the ITU hosts study groups and arranges global and regional events and workshops that are open to non-members. The ITU hosted the World Summit on Information Society (WSIS), which was held in two phases in 2003 and 2005. This resulted in the Geneva Declaration of Principles and the Geneva Plan of Action (2003), as well as the Tunis Commitment and the Tunis Agenda for the Information Society (2005).[551] These documents provide principles and target goals on the development of the global information society. A related actor is the Internet Governance Forum (IGF), whose purpose is to support the UN Secretary-General in carrying out the mandate from the WSIS with regard to convening a forum for multi-stakeholder policy dialogue.[552]

The Organisation for Security and Co-operation in Europe (OSCE) offers a platform for discussion, dialogue and practical work on security issues.[553] The work of the OSCE has a broad approach, taking into account not only military security matters, but also economic, environmental and human issues. This is an advantage for addressing cross-dimensional, transnational threats which is consistent with addressing cyber threats. The cyber security aim of OSCE is traditionally focused on individual aspects such as combating cyber crime and the use of the internet for terrorist purposes but, in 2011, it was expanded to include direct discussions on possible Confidence Building Measures (CBM) with PC Decision 1039. A restructuring of the OSCE Secretariat in 2011/2012 saw the new Trans-National Threats (TNT) Department directly assume responsibility for 'threat emanating from the misuse of ICT', which currently supports the PCD 1039 process. The TNT Department also includes two organisations which previously dealt with international cyber security issues from their respective mandates: the Action against Terrorism Unit (ATU)[554] and the Strategic Police Matters Unit (SPMU).[555]

The Organisation for Economic Co-operation and Development (OECD) was founded to stimulate economic progress and world trade.[556] It offers capacity building activities that are also open to non-Member States that participate as observers. The OECD hosts a number of committees that discuss and review policy development in specific areas. The work of the committees may result in multilateral agreements, standards and models, and recommendations and guidelines. Several committees,

---

551 For all official documents and more information about WSIS, see: http://www.itu.int/wsis/index.html.

552 Internet Governance Forum: http://www.intgovforum.org/cms.

553 Organisation for Security and Co-operation in Europe: http://www.osce.org.

554 Action against Terrorism Unit: http://www.osce.org/atu.

555 Strategic Police Matters Unit: http://www.osce.org/spmu.

556 Organisation for Economic Co-operation and Development: http://www.oecd.org.

in particular the Committee on Information, Communications and Computer Policy (ICCP), have contributed to analysis of policy development within the cyber arena.

Commitments regarding these organisations and others are followed by implementation which, in turn, may demand measures to be taken by states. These come with a price, as they may require the establishment and/or reorganisation of public institutions and agencies. There are also likely to be demands for new methods and processes. Requirements for new capabilities, technical development and education are only few examples of consequences for states that want to participate in the benefits of cyberspace.

Due to the advantages offered to society by the digital environment, such investments continue to be made. State caution on entering into commitments, on the other hand, is increased due to fears of over-regulated and limited freedom of action. These constraints come with the acceptance of new obligations related to cyberspace and must be measured against the expected advantages of a given commitment.

The growing importance and, indeed, the integral nature of ICT to core societal functions must be taken into consideration. This is a strong consideration when states examine their options and freedom of choice regarding activities in cyberspace. For example, membership in ICANN is optional. There are no formal obligations for states to become members of this organisation. Yet it is not a plausible strategy for states to ignore the existence and activity of such an organisation. This is compared with the ITU (some of whose activities could overlap with ICANN) whose membership is essentially mandatory as it comes with UN membership. Yet, even in this case states are free to choose the level of engagement with and investment into the organisation.

Due to the inherent features of the digital society, where vulnerabilities can be widespread and interdependency is high, information sharing can offer advantages to the handling of cyber threats. Cultivating this skill and formalising its performance within an organisation can provide better preparedness and improved incident response capabilities. However, this is generally a voluntary arrangement, which in turn presupposes an element of trust. One mechanism for building trust (and other measures) at the state level is the establishment of Computer Emergency Response Team (CERTs) and Computer Security Incident Response Team (CSIRTs), but only when these organisations are seen as being responsive to legitimate cooperation requests, and generally counting as 'trust actors' within accredited peer groups (such as the FIRST network). Information sharing[557] or building connectivity

[557] For a further discussion on information exchanges, see Section 4.

between stakeholders at an international and national level between CERTs/CSIRTs and governments is critical for the protection of critical infrastructure (and critical information infrastructure). As operational-level CERTs/CSIRTs information sharing continues to increase, improvements must also continue to be made, particularly between CSIRTs with national responsibility.[558] Information sharing (also described as Information Exchanges) is increasingly being driven by public-private partnership models, even within international contexts.[559] Cross-border information sharing mechanisms are crucial to managing a crisis and mitigating incidents, in particular, those that could spread quickly beyond the capacity or ability of the local operational CERTs and impact delivery of critical infrastructure services.[560, 561]

### 5.3.2. Assurance Mechanisms: Information Security

A principle of all government activity is quality assurance – a component of quality management that is 'focused on providing confidence that quality requirements will be fulfilled.'[562] This is ensured through specific business processes, design principles and risk management criteria that ultimately form the bedrock of information security in general, and NCS in particular.

Information Security (which is often used interchangeably with the phrase information assurance, although the latter is a considerably wider concept) is often directly equated with cyber security, and forms the critical process-orientated assurance component in delivering cyber security for any organisation.

Information Security is generally defined as the ability to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.[563] This is accomplished through a process of Information Security Management that defines a 'security target' – such as a specific file, a computer, a system or an entire organisation. This

---

558 One such group is the European Government CERT Group.

559 On example for an international PPP is the European Public Private Partnership on Resilience (EP3R) of the European Commission.

560 European Network and Information Security Agency, (ENISA), NATO Computer Incident Response Team (NCIRC), Task Force – Collaboration of Computer Incident Response Team, (TF-CSIRT), Forum of Incident Response and Security Teams (FIRST) is an organisation for sharing best practice information.

561 On information sharing, the International Watch and Warning Network (IWWN) is another example of an organisation states are free to join. The purpose of the IWWN is to coordinate the efforts of national CERTs and government agencies as well as to offer informal globally operating consultation in the event of cyber incidents. Its members are AZ, CA, FI, FR, DE, HU, IT, JP, NL, NZ, NO, SW, CH, UK, US.

562 AS/NZS ISO 9000:2006, 'Quality management systems – fundamentals and vocabulary,' 9.

563 For a general presentation on the topic see Bodgan Mosneagu, Edgardo Vasquez, and Jay Lam, 'Information Security as a Profession,' (2012).

security target is then protected according to a specific protection requirement or protection profile, which will address basic information security principles of that target. The most basic of such security principles are confidentiality, integrity and availability (C-I-A)[564] but further principles can be added as required.

Information Security Management is closely connected with a number of steps, in themselves related to the process of Risk Management. Using the ISO 27002 series structure as a point of departure, this includes:[565]

**Risk assessment:** a thorough evaluation of the various 'attacks' (which includes intentional and unintentional acts of human and natural origin) that a system can be subjected to. Risk assessment (also known as risk analysis) is a very in-depth process that often is software-supported[566] due to the large number of attacks (often numbering in the thousands) and their cross-linkages that need to be considered.

**Security policy:** this includes general guidelines to be aware of, ranging from such issues as how to deal with 'Bring Your Own Device' up to the granting of administration rights to desktop clients, or rules about which websites can be accessed.

**Organisation of information security**: this includes the specific assignment of roles (such as system administrator or auditor) and responsibilities (such as setting access privileges) for the organisation as whole. In particular, this also defines who will be responsible for ensuring that the Information Security Management process is adhered to.

**Asset management:** this includes inventory and classification of information assets – usually physical, such as in hardware or in computer peripheries. Asset Management often also connects to the critical issue of 'trusted supply chain' – the protection of hardware from intentional interference.

**Human resources security**: in government, this includes the handling of relevant personal security clearances and ensuring that this process is connected to information security. This becomes a particular issue with regard to special compartmentalised information.

---

564 See also Section 1.2 and 3.1 for further discussion of the C-I-A triad.

565 ISO/IEC 27001:2005, 'Information technology – Security techniques – Information security management systems – Requirements.'; ISO/IEC 27002:2005, 'Information technology – Security techniques – Code of practice for information security management.'; ISO/IEC TR 27008:2011, 'Information technology – Security techniques – Guidelines for auditors on information security controls.' For an introduction see: http://www.27000.org.

566 A wide range of software-supported risk analysis systems exist, including the BSI *Grundschutz*, EBIOS, CRAMM and a number of others.

**Physical and environmental security:** this refers to building and perimeter security from both a safety and security perspective. In information security, electronic emissions mean that often a secure environment has to extend outside of the immediate physical vicinity. Buildings themselves can be TEMPEST[567] proof, but other considerations (such as regarding the nature of electric power supply) need to be taken into account.

**Communications and operations management**: this is the 'heart' of much of cyber security, and includes defining the responsibility for the management of technical security controls in systems and networks including, for instance, firewalls and similar tools.

**Access control:** usually working in conjunction with human resources security, access settings are a critical in determining who has the right to access what part of a computer network, system, application or data. Traditionally, many of the most serious breaches of information security have come through errors in access control – particularly regarding expired accounts of former employees.

**Information systems acquisition, development and maintenance:** in general closely associated with Asset Management, this function is often split in larger organisations, sometimes repeatedly, as it includes, in essence, three separate tasks. Acquisition, in particular, is often a highly sensitive issue, particularly with regard to compartmentalised networks.

**Information security incident management:** this function includes the entire scope of 'cyber crisis management' (also known as business continuity management or as continuity of government), which itself encompasses a large set of procedures normally dealt with separately. This component also includes disaster recovery – usually meaning the separate storage and treatment of relevant data.

**Compliance:** this function details the roles and responsibilities of the monitoring process, as well as ensuring that other relevant standards and regulations are adhered to.

The above categorisation is intended to be scalable, and thus applies equally to very small and very large organisations. In fact, each of the above sections will normally amount to an entire organisation, or even a number of different organisations, within a governmental structure.

---

567 TEMPEST involves shielding an object from spurious electronic emissions (see SANS Institute, An Introduction to TEMPEST, (Bethesda, ML: SANS Institute, 2012), http://www.sans.org/reading_room/whitepapers/privacy/introduction-tempest_981.

The importance of having a government-wide Information Security Management System (ISMS) cannot be overemphasised. There is no chance of even a basic level of cyber security if these protection matters are not dealt with in an encompassing and systematic fashion. This does not mean that, for instance, all government departments must use a single specific ISMS, or even that within a single department only one specific ISMS is used. It does, however, imply that every ISMS in use should be put into a relationship with other, 'neighbouring' ISMS and that, overall, for each 'measurable unit' (be that a system or a department), there is a closed loop within the basic Plan-Do-Check-Act cycle.[568] As the results of each of these ISMS must be able to communicate with each other, widely-shared frameworks (such as the 'Common Criteria Approach') can be useful.

The 'Common Criteria Approach' represents the outcome of efforts to develop criteria for the evaluation of IT security which are widely used within the international Information Security community. It is based on an alignment with, and development from, a number of source criteria, including the existing European, US and Canadian criteria (Information Technology Security Evaluation Criteria (ITSEC); Trusted Computer System Evaluation Criteria (TCSEC); Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), respectively). It is a contribution to the development of an international standard, and opens the way to worldwide mutual recognition of IS evaluation results.[569]

Common Criteria processes are particularly useful as a driving force for the mutual recognition and adoption of secure IT products. By using a Common Criteria framework, users can develop a common understanding of their security requirements (their protection profile) and communicate these to vendors, who can implement the relevant security attributes in their products, which can further be independently tested and evaluated. Thereby, Common Criteria provides for a basic level of assurance in international information security. To a limited extent, and in conjunction with relevant consumer protection legislation, this can help to shift liability to vendors and producers, albeit only within a narrowly-defined context. In addition, standards guide and assist consumers in defining their requirements. Purchasers of computers and information security systems representing the public sector also benefit from this system but, in order to take full advantage of it, they need to ensure an effective application of the Common Criteria (e.g., by specifying what *functions* and not what *products*, are of interest). Common Criteria can, therefore, be a powerful tool in promoting international cyber security.

---

568 Also known as the 'Deming Cycle' (see, for instance, Paul Arveson, 'The Deming Cycle,' Balanced Scorecard Institute, http://www.balancedscorecard.org/TheDemingCycle/tabid/112/Default.aspx.).

569 See Syntegra, 'Common Criteria. An Introduction,' NIAP, http://www.niap-ccevs.org/cc-scheme/cc_docs/cc_introduction-v2.pdf.

No certification or understanding of business information characteristics can reduce risk to zero. There will always be an element of residual risk. To protect everything is very difficult to accomplish and, as high-profile attacks proliferate, there is a growing move towards an 'assumption of breach'.[570] In other words, a public or private sector organisation should design their cyber security systems in the implicit knowledge that targeted attacks are likely to successfully breach those systems. A key question is: which elements of its information inventory should an organisation protect at all costs? This question will be difficult to answer, as the cost of maximising the protection applied to information will likely result in it being less accessible for its original purpose.

## Delivering Improvements

Development and improvement of national cyber policy can occur across three main areas: (1) within government organisations, (2) in cooperation between the public and private sectors, and (3) outside of government. One significant variable running through these areas is the balance of power between actors. For example, government has significant leverage in delivering improvements in the first area – working within and across the public sector. Improvement of national cyber policy is, in large part, dependent on organisational mandates, and central government leverage comes in large part through the division of responsibility. Overlapping or conflicting mandates tend to encourage inertia and exacerbate inter-departmental tensions, leaving policy gaps that can be exploited.

Allocation of resources is another familiar tool for driving change. Cyber-related resources (e.g., money, people or political support) are often directed towards organisations that already hold related mandates (e.g., security services and/or the military). As long as resource allocation can be linked robustly to a strategic (i.e., long-term) plan, it can be an effective tool for driving cyber policy improvements. Governments will also be aware that allocation of resources is likely to be time-consuming; especially if it involves new or expanded organisations (which will themselves need to develop a plan to metabolise and prudently spend taxpayer money).

Governments acknowledge the importance of working with the private sector in the construction and management of the (largely privately-owned) networks upon which they and their populations rely. A significant challenge is to shift this cooperation beyond its current transactional mode and towards a model that integrates the respective strategic strengths of these powerful organisations. It comes as a surprise to many officials to realise that the private sector has a vast

---

[570] Brian Prince, 'NSA: Assume Attackers Will Compromise Networks,' *eWeek.com*, 17 December 2010.

amount of data about the network traffic that passes over its systems and is able to develop outstanding intelligence about the capabilities and activities of users. Executives representing key ICT corporations/service providers often publicly comment that they would welcome improved cooperation with governmental institutions – state institutions often work hard to generate information that could be made available to them at low cost and enhanced with private sector cooperation. Improvements can be driven outside government, with government entities encouraging – from a detached perspective – cyber security progress in the private sector. Economic incentives can be calibrated according to specific sectors and, from a broader perspective, governments can make progress with setting the right 'system defaults' that permit possibilities for future innovations. A more nuanced understanding is needed, in government and in wider society, of the modern digital environment (e.g., technological diffusion, the dramatic increase in connected users and devices, etc.). This will help to place NCS measures in the proper perspective – as a means to a specific end (e.g., as a means to the larger social and economic goals sought by all governments). Governments that can adapt internally to increase their compatibility with rapidly changing economic and technological environments will reap the rewards of greater competitiveness and prosperity.

## 5.4. NATO'S CYBER DIMENSION

Digital communications are the backbone of society and, whilst they are a capability that NATO exploits for operational and administrative advantage, it is neither an environment that NATO, nor its Member States, can claim to control. The ability to collect, process and deliver vast amounts of data requires huge increases in military and bureaucratic efficiency. At the same time, all NATO nations need to work with the fact that their dependence on cyberspace, including the internet, is a major vulnerability and, unless invested in, will result in deteriorated overall resilience.[571] NATO, the armed forces, International Organisations (IOs) and Non-Governmental Organisations (NGOs) that work with it expose themselves to known and unknown risks while operating in the digital domain. Business as usual for NATO includes the procurement and organisation of military capabilities, engaging in the political processes that support the operation and coherence of the North Atlantic Council, and the administration and control of the NATO command elements and forces assigned to NATO activities. It is a huge undertaking with operational, logistic, economic, political, technical, environmental and reputational risks.

The Alliance is inextricably linked to the digital domain and is faced with many threats that create problems for Member States since cyberspace is international

[571] Melissa E. Hathaway, 'Toward a Closer Digital Alliance,' *SAIS Review* 30, no. 2 (2010).

by nature. The interconnectivity makes a weakness of one country a weakness in all, which means that states and organisations cannot deal effectively with cyber threats on their own.

To tackle these challenges, NATO endorsed the 'in-depth cyber defence' concept at the Lisbon Summit 2010,[572] a strategy which cuts across a variety of stakeholders and implicitly embraces the Whole of Government approach, due to the fact that the lead responsibility of cyber defence in most nations resides in civilian agencies and with non-governmental actors. In 2010, NATO presented its latest Strategic Concept which recognised the growing international significance of cyber security, both as an issue for NATO to address in terms of capability, and as a challenge in respect of NATO's future international relevance.[573] The strategic concept was followed by the 2011 Policy on Cyber Defence (and associated Action Plan) which directed the defence of NATO systems as well as placing a responsibility on Alliance Members to protect their own critical networks.[574]

Functionally, NATO has only responsibility for its own computer networks, not for the networks of Allies. The most important operational body to protect these networks – the NATO Computer Incident Response Capability (NCIRC) – was established in 2003 and expanded in 2011-12. In particular, this has led to an increase in the forensic capability analysis – a function that can also be provided to NATO member countries and partners as needed.

There are different opinions about whether a major cyber attack could overwhelm a state and reach the threshold of Article 5 of the North Atlantic Treaty, requiring collective defence measures.[575] So far, the predominant view is that the risk that this will occur is low. However, there is an expectation that a significant attack could result in a NATO Article 4 discussion. What is not clear is what that discussion would look like, depending on the extent of damage, the degree of certainty regarding evidence, and to what extent political leaders would have to rely on 'security bureaucrats' to interpret events and formulate responses.

### 5.4.1. NATO's Collective/Cyber Defence

The North Atlantic community came together in 1949 to create NATO, pledging to come to each other's defence when called upon. This collective defence, enshrined in Article 5 of the Washington Treaty, also applies to cyber security – but not under

---

572 NATO, *Lisbon Summit Declaration* (Lisbon: NATO, 2010).

573 NATO, *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation* (Lisbon: NATO, 2010).

574 NATO, *Defending the networks. The NATO Policy on Cyber Defence.*

575 See United States et al., *North Atlantic Treaty.*

all conditions. Within the context of using the 'five mandates' model of NCS[576] this means that it does not apply across all five of the NCS mandates.

NATO first suffered significant cyber attacks in 1999, during operation ALLIED FORCE against Serbia, with a number of variously entitled 'patriotic hackers' conducting denial of service attacks and webpage defacements.[577] As these attacks were relatively minor they were primarily an issue for the 'counter cyber crime mandate' of NCS, and not one for 'collective defence', no matter how interpreted. Even the 2007 cyber attacks against Estonia did not trigger an Article 5 response. Despite the severity of those attacks, it was not considered to have actually crossed the line where military collective defence would be necessary. As with the 1999 incident, the 'military mandate' did not come to the fore, although nations did provide technical and policing assistance relevant to other mandates.[578] However, NATO has decided that its 2007 response to Estonia was too limited, and has since sought to expand both its capabilities as well as its strategic and operational procedures in this area.

NATO made clear in the Policy on Cyber Defence[579] that collective defence does apply in cyberspace, and even discusses the process the Alliance will use to invoke collective defence – while maintaining ambiguity about specific thresholds. This process for escalation begins at the tactical (technical) level. If an incident has political implications for collective defence, the incident would get escalated up through respective technical and policy levels to the North Atlantic Council.[580] The process for Article 4 consultations in case of a serious cyber attack has also already been especially addressed.[581]

As part of the dual concepts of 'smart defence' and increased 'pooling and sharing', NATO has stipulated for the possibility of deploying a NCIRC Rapid Reaction Teams (RRT)[582] to assist Alliance Members in their efforts to deal with cyber-related incidents. The deployment request may be politically or strategically originated; the deployment of these teams may assist a country resolve a technical issue, or the team may be able to collect independent evidence as to the nature and

---

576 These mandates include (1) Military Cyber (2) Counter Cyber Crime (3) Cyber Diplomacy and Internet Governance (4) Intelligence & Counter-Intelligence (5) CIP and Crisis Management. See Section 1, Section 4.

577 For more details, see Healey and Bochoven, 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.'

578 Ibid., and Healey et al., *Building a Secure Cyber Future: Attacks on Estonia, Five Years On [Transcript].*

579 NATO, *Defending the networks. The NATO Policy on Cyber Defence.*

580 For more details, see: Healey and Bochoven, 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.'

581 NATO, *Defending the networks. The NATO Policy on Cyber Defence.*

582 NATO, 'NATO Rapid Reaction Team to fight cyber attack,' *NATO Newsroom*, 13 March 2012.

possible cause of the incident. Another step taken is the establishment of the NATO Communications and Information (NCI) Agency,[583] a result of the merger of the NC3A, NACMA, the ALTMB Programme and the NATO Headquarters.[584] The NCI Agency will provide NATO with IT and C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). Finally, a proposed 'Cyber Red Team' (CRT) has been under discussion since a number of years. The CRT is intended to conduct penetration testing of NATO's own systems, but could theoretically be employed to support NATO Members and partners.

These developing NATO capabilities should not be seen as absolving an Alliance Member from taking all reasonable steps to protect their capabilities, ensure their resilience, and expedite their recovery after attack. The 2012 Chicago Summit Declaration stresses the overall commitment to improve the protection of NATO digital assets, and the further integration of cyber defence measures into Allied structures and procedures.[585] However, NATO nations are increasingly making it clear that they view the subjects of NCS and (collective) cyber defence to be closely interconnected. The White House has said this most directly, saying: 'All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.'[586] Other national strategies typically mention NATO commitments but not directly collective defence, such as the French NCSS: 'strong relations between allies form the basis of an effective cyber defence policy.'[587]

Exactly what 'collective cyber defence' may entail is not necessarily clear, and can cover a very wide range of cyber-specific actions. These could include:

- Using the military or civilians to help defend critical infrastructures in an affected nation,
- Using military or civilians to help on crisis management tasks, from the easiest (note taking and call management) to professional incident responders to lead incident response,

583 See: http://www.ncia.nato.int/Pages/default.aspx.

584 NATO Consultation, Command and Control Agency (NC3A), The NATO ACCS Management Agency (NACMA).

585 NATO, *Chicago Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012.*

586 White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*: 14.

587 French Secretariat-General for National Defence and Security, *Information systems defence and security. France's strategy*: 18.

- Deploying forensic investigators to assist the investigation,
- Deploying teams or other groups to assist with coordination with NATO or other nations or sectors. For example, a representative of the FS-ISAC[588] could travel to the country to help information flow on attacks to finance; or a military liaison team could do the same for military coordination,
- Ordering (or convincing) Internet Service Providers (ISPs) to block attack traffic destined for the nation under attack,
- Ordering (or convincing) ISPs to throttle traffic to the nation suspected of being behind the attack until they cooperate in helping to end the attack,
- Active defences to selectively disrupt Command & Control infrastructure behind the attack,
- Build additional local Internet Exchange Points and other local infrastructure to help them weather the attack and increase their defensive options,
- Ordering or otherwise ensuring that manufacturers of networking gear prioritise shipments to the country under attack to help them build additional capability,
- An Alliance Member deploying its own offensive cyber forces to engage in counter-attacks on behalf of the Alliance.

Given the ambiguity involved in the term 'collective cyber defence' (indeed, the term itself is not officially used within NATO) there is no reason to believe that retaliatory actions would not be 'cross-domain', i.e., occur outside of cyberspace. However, if interpreted narrowly, collective cyber defence offers also other interesting possibilities: as much of it could become active without Article 5, this leaves the possibility open that NATO could engage in 'collective cyber defence' with non-NATO nations as well.

588 The Financial Services Information Sharing and Analysis Center (FS-ISAC) is one of the oldest, largest, and most successful information exchanges in cyber security. Founded in 1999, FS-ISAC has 12 of the largest US banks as well as other critical financial institutions as its members.

## 5.4.2. Cooperation with Non-NATO Nations

In recent years, NATO has considerably expanded its remit for cooperation with non-NATO nations. In the fall of 2011, Austria became the first country to enter into a specific bilateral cooperation scheme managed by the NATO Emerging Security and Challenges Division (ESCD), focusing on 'all relevant aspects of cyber security.'[589] Since then, a half-dozen other nations have signed similar agreements with NATO.[590]

Bilateral cooperation agreements of this nature can include a whole range of different options: harmonisation of crisis management procedures; exchange of relevant information and assessments; mutual inclusion in research projects; joint mentorships in third countries to raise awareness; development of joint 'lessons learned' processes, including cyber aspects of crisis management operations; establishment and enhancement of cyber security related capabilities and procedures; training and exercises (including participation at the NATO Cooperative Cyber Defence Center in Tallinn), and the involvement of the private sector, as appropriate.[591]

Besides specifically tailored bilateral programmes for selected Partnership for Peace (PfP) and possibly Mediterranean Dialogue Program (MDP), and Istanbul Cooperation Initiative (ICI) nations, NATO is also reaching out via established instruments and policy proposals. Some parts of NATO's Cyber Policy and Action Plan are open to non-NATO nations. Recent suggestions have been tabled that would see the Individual Partnership Cooperation Program (IPCP), the Planning and Review Process (PARP) and the Science for Peace Studies Programme (SPS) significantly expand their cyber security focus. As these programmes represent some of the main programmes for non-NATO nations, the strengthening of the cyber security dimension could have a significant impact on the overall relationship of NATO to these countries.

NATO may also choose to run specific projects to improve the cyber preparedness of its Alliance Membership and other allies as part of Mediterranean Dialogue, Partners for Peace, or the Istanbul Cooperation Initiative. Where systemic weakness in critical cyber infrastructure creates critical national vulnerabilities, the nations themselves or NATO may consider compensatory measures to reduce the residual risk.

---

589 Gerhard Jandl, 'The Challenges of Cyber Security – a Government's Perspective,' *Human Security Perspectives*, no. 1 (2012): 36.

590 Ibid.

591 Ibid.

### 5.4.3. NATO-EU Cooperation

There is a rough consensus[592] that NATO and the EU Institutions should work together to create an environment where a single set of security and resilience standards are promoted, and where there is coherence between societal, economic and national security strategies. Operational level discussions have been partially hampered by the significantly different focus of both organisations – the operational capabilities of NATO and the regulative capabilities of the EU both have virtually no commonality in the each other's organisation.

Cooperation between NATO and the EU was institutionalised in the 2003 Framework for Cooperation, which still is the basis for most common efforts. Regular meetings occur at all levels from the tactical to the political. There are regular staff contacts at all levels between NATO's International Staff and International Military Staff, and their respective EU interlocutors (Council Secretariat, European External Action Service, EU Military Staff, European Defence Agency, Commission, European Parliament, etc.). Permanent military liaison arrangements exist to especially facilitate cooperation at the operational level. A NATO Permanent Liaison Team has been operating at the EU Military Staff since November 2005 and an EU Cell was set up at SHAPE (NATO's strategic command for operations in Mons, Belgium) in March 2006.[593]

Within the EU Common Foreign and Security Policy (CFSP) framework, one of the most significant agreements the EU and NATO have is the 'Berlin Plus' agreement.[594] In effect, the agreement guarantees that the EU has the right to expect the support of NATO facilities, staff, and even deployed equipment in case of a 'crisis management' CFSP mission – but only if NATO does not require the same resources. Particularly important for cyber defence was that the agreement also regulated the exchange of confidential information.[595] Since the agreement, NATO and the EU have expanded cooperation on a range of other issues, including counter-proliferation, counter-terrorism, and general capability development. NATO cooperation with the European Defence Agency (EDA) has been expanded in recent years, and EDA has defined cyber defence as a priority within its overall Capability Development Plan.

---

592 See, for instance, Reyhaneh Noshiravani, 'NATO and Cyber Security: Building on the Strategic Concept,' *Chatham House Rapporteur Report*, 20 May 2011.

593 See: NATO, 'NATO-EU: a strategic partnership, 'http://www.nato.int/cps/en/natolive/topics_49217.htm.

594 Tim Waugh, 'Berlin Plus agreement,' European Parliament, http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/berlinplus_/berlinplus_en.pdf.

595 See: EU-NATO, *The Framework for Permanent Relations and Berlin Plus* (Brussels: Council of the European Union, 2003).

The discussion on what framework would work best for NATO-EU cooperation on cyber security has been ongoing for many years: some favour specifically-expanded 'Berlin Plus' arrangements, others would like a specific comprehensive agreement. In fact, the current NATO-EU cyber cooperation is already partially regulated by existing agreements – there will certainly be some form of cooperation between the NATO NCIRC and the CERT-EU, for instance. The expansion of this cooperation into other areas – in particular counter cyber crime and critical infrastructure protection (CIP) – is contentious due to concerns regarding NATO's actual mandate in these areas, the status of EU non-NATO nations, as well as data protection issues.[596]

### 5.4.4. The NATO Defence Planning Process

The NATO Defence Planning Process (NDPP) is one of the principle tools of the Alliance, intended to enable member countries to benefit from the political, military and resource advantages of working together. Within the defence planning process, Allies contribute to enhancing security and stability, and share the burden of developing and delivering the necessary forces and capabilities needed to achieve the organisation's objectives. Crucially, the NDPP is intended to 'prevent the renationalization of defence policies, while at the same time recognizing national sovereignty, inter. operability between Alliance members as well as guaranteeing a certain level of overall efficiency.'[597]

The NDPP is composed of a number of specific procedural 'steps' as well as a number of Alliance – based supporting institutions and committees.[598] It has been repeatedly stated that cyber will be added to the NDPP, in particular through the 'building of resilience',[599] although no details have been made public.

The possible repercussions of including cyber within the NDPP are considerable. One of the most important aspects of the NDPP was the 'burden sharing' arrangement regarding specific defence infrastructure. Under the NDPP, for instance, NATO was able to largely directly finance the construction and maintenance of crucial airbases in northern Norway during the Cold War. Given that the vast majority of cyberspace infrastructure is privately held, it is not clear how NATO could help build Alliance capabilities through a direct financing effort, as was done with basing infrastructure. Nonetheless, as there is likely to be Alliance funds available, it can be presumed that a solution will be found to this dilemma as well.

---

596 Brian Beary, 'As momentum for action builds, EU's role remains unclear,' *Europolitics*, 3 May 2012.

597 See: NATO, 'The NATO Defence Planning Process,'http://www.nato.int/cps/en/natolive/topics_49202.htm.

598 For a full list, see ibid.

599 NATO, 'Cyber defence: next steps,' *NATO Newsroom*, 10 June 2011.

## 5.5. CONCLUSION

One relevant question for policy-makers remains: why should they invest resources in the commitments, mechanisms and governance required by a NCS strategy? After all, the majority of investments in this domain will require trade-offs; very few are cost-free. The answer is provided by the potential benefits that accrue to states that develop a coherent NCSS. A governmental strategy is necessary for dealing with the myriad digital issues that confront policy-makers in the 21st century. The benefits of connectivity are too great to ignore, and policies that can deliver these benefits in a safe and secure manner can bring a significant return on investment. Without communicating a strategy which contains goals as well as expectations, the efforts made are at risk of being uncoordinated and without sufficient coherency, thereby at risk of diminishing their original effects.

The development of national cyber security policies – and the process of constructing and navigating cyber-related commitments, mechanisms and governance structures – is inherently about trade-offs. But not all trade-offs are similar and some will change the course of a nation. Failing to achieve the societal or the economic potential available through digital technologies could – over time – relegate a previously successful state to a junior division in a league of nations.

It can be tempting to isolate cyber risks from the broader environment – to treat them separately, perhaps behind closed doors, in a manner that is less transparent than that of other societal risks. This approach misses the point that cyberspace is a thin, but highly conductive layer that complements nearly all facets of daily life for most people around the world. It has permitted the spectrum of human activities to be transposed into a digital environment. This includes many positive actions but it also encompasses crime, espionage, terrorism and warfare. These activities may take on different capabilities in the digital age, but their essential nature remains the same.

As complex bureaucracies and social systems have evolved in order to deal with all the issues that face a modern state, so too will complex approaches be required to deal with the problems that will permeate the new century. The digital environment is evolving rapidly – yet creating law is a lengthy process. All legislation is based on political will which, in turn, is shaped by social and economic forces. What are needed are more approaches that link policy-makers around the world, in the same manner as the issues are linked. Increased compliance does not necessarily equate to increased security. States need to be active and take necessary action on the information they possess. Information-gathering alone will not be sufficient. In areas where the process of alignment – between policy-makers and issues – has taken place, there will be a need for a system of capturing and preserving useful

knowledge. This lessons learned process (or more modestly, 'lessons identified'), will become increasingly critical as more nations develop cyber security policies.

Ingenuity in the digital age is thankfully in abundant supply, and significant amounts of human capital are focussed on delivering cutting-edge capabilities. By comparison, very little capacity is being used to address the security considerations that accompany technological development. It is critical that knowledgeable policy-makers are cultivated across the public and private sectors, who are able to understand the complexity and ambiguity created by the cyber layer, and how it affects the delivery of current and future objectives. NATO's primary challenge is to decide the role it will play in the global cyber ecosystem, develop its capability to operate – even in a cyber degraded environment – and delineate responsibilities between the command structure and Member States.

## 5.6. TACTICAL/TECHNICAL PITFALLS, FRICTIONS AND LESSONS IDENTIFIED

**Under/Overvaluing International Commitments:** national law should always be the defining element behind any governmental cyber security instrument. International law, both soft and hard law, is however less likely to play a less rigorous role in defining national approaches. This is largely due to the as yet embryonic understanding of cyber conflict, and the exact role that international treaties, in particular the Law of Armed Conflict, have in this domain. This even more important when assessing the possible behaviour of other nations in cyberspace: building a cyber security system that completely depends on foreign cooperation in case of attack, for instance, could well find itself short of critical capabilities when it needs them. At the same time, ignoring or undervaluing international commitments could further weaken attempts aimed at creating international normative frameworks for cyber security.

**Failing to understand Information Security requirements:** cyber security is impossible without the implementation and provision of in-depth Information Security Management Systems (ISMS) that are applied across an organisation in its entirety. The implementation of an ISMS system can cause considerable disruption to traditional business practices, and thus this can this be one of the most difficult tasks to accomplish in a NCSS. It is, however, one of the most crucial: without a single overarching ISMS (or a seamless integration of multiple ISMSs) it is impossible to provide for the even the most basic protection of government systems.

**Lack of International Interoperability:** interoperability in cyber security is a must. Unlike, for instance, traditional territorial defence, it is very difficult for a nation

to defend itself against major cyber threats purely with its own governmental means. Interoperability means that government cyber security staff must be able to cooperate not only with other governments, but also with non-state partners. In particular, it means sharing a similar skill base and overall knowledge level as the international partners – and, optimally, a similar appreciation of threats as well.

**Ignoring Lessons Identified:** as a relatively new and very quickly evolving field, the role of lessons identified (and, optimally, lessons learned) in NCS is a vital one. Very often the initial legal and organisational responses to a specific cyber threat will turn out to be inadequate, or obsolete in the face of technical and social change. Sharing experiences between different organisations nationally and internationally is a very important way to communicate answers as well as identifying the underlying issues. Ultimately, the ability to rapidly adjust systems, processes and even regulations and legislation is the only way to 'future-proof' any NCS system.

# 6. CONCLUSION

## 6.1. THE ROAD SO FAR

'Essentially, all models are wrong, but some are useful.' The famous quote of George E. P. Box was originally applied to statistical models, but it could be said to be at least as applicable to describing models of national cyber security. The very term 'national cyber security' (or NCS) is hardly ever defined in official publications, although the term itself is certainly in widespread common usage. Even the spelling of the word 'cyber security', let alone its definition, is contentious. The same lack of clarity applies to many of the constituent terms of NCS, and, indeed, can be said to be representative of the domain of cyberspace itself: there are few terms, let alone models, that will not be contentious. Therefore, the goal of this publication, namely to inform readers of the various factors to consider when drafting a NCS, can only partially be achievable.

A basic assumption of this publication is that there is no such thing as a single perfect framework for national cyber security. Each individual system of government will provide its own particular set of circumstances that need to be addressed, and each particular strategy will wish to emphasise individual mandates. In an optimal world it would be possible to view the entire process of creating a national cyber security strategy (or NCSS) as being composed of a step-by-step process – but in reality any such process is likely to be more impromptu. Therefore, the most important contribution this document can offer is to raise awareness of the most critical issues in a NCSS – and how they can be defined.

Unlike other publications that have sought to inform policy-makers on the options available in drafting a NCSS, this publication does not concentrate solely on a set of specific tasks or elements that must be delivered for a NCS to be considered useful (e.g., 'information exchange', 'public-private partnerships', etc.). While this approach has its own validity, it is especially designed to explain NCS from one particular viewpoint – for instance, one that emphasises, say, critical infrastructure protection – and concentrates on the 'ten most important tasks' needed to accomplish this goal. This type of approach may succeed in communicating a particular view of NCS, but does not provide the reader with an all-round view of the various options and their consequences. Moreover, such an approach is usually specifically targeted at a certain level or type of policy-maker, to exclusion of all others. This contributes to the overemphasis on a specifically selected process, and an unquestioning assumption of definitions and concepts. In short, it does not provide the more strategically-minded or critical reader with the actual strategic context in understanding what, exactly, NCS could entail. This is especially problematic as context is absolutely

central to any interpretation of NCS. There are no purely descriptive approaches to the subject – either implicitly or explicitly, all views on NCS are informed by a specific theoretical approach.

Theoretical approaches to the subject are, therefore, not optional; they are mandatory in order to frame a country's particular brand of NCS. Further, these frameworks need to be applied to the correct level of conceptual understanding as well as organisational responsibility within a governmental structure – this document, after all, is focused on a governmental view of the subject. Conceptually, one hierarchal model is to see policy clearly developing in a 'top-down' fashion: the national security strategy (e.g., the Dutch 2008 National Security Strategy) informs the national cyber security strategy (e.g., Netherlands NCSS 2011) which outlines a set of specific organisations (e.g., the Netherlands National Cyber Security Centre) which each have sub-organisations and specific tasks attached to it (e.g., a Computer Emergency Response Team, or CERT). The levels of responsibility articulated in this model correspond to the different sections of the present publication: the political (Section 2), strategic (Section 3), operational (Section 4) and tactical (Section 5).[600] The sections can also be read independently, or as a group – it is up to the reader to decide which level of detail is required, and at what level.

The core theoretical approaches of this publication are directly applicable to the various levels of policy development. They reflect what the authors consider here to be the 'essential truths' of the NCS domain. These read as follows:

1. **The multifaceted nature of National Cyber Security (the 'Five Mandates'):** as is shown in detail in Section 4, NCS tends to be interpreted differently in the five specific fields of government endeavour that comprise the operational level of NCS.[601] These five views, or mandates, have developed historically and often in relative isolation from each other. They each have differing goals, organisational structures, and even specific definitions associated with them. Policy-makers need to be aware that most initial attempts at formulating a NCSS will, by default, only address a few of these mandates from the outset. NCS is an enormously complex subject, with a number of different interpretations, depending on the viewpoint of the observer. By applying a variant of the incident management cycle to the five mandates, it is possible to show where most mandates will be active (and have specific

600 Properly, the section is really intended to address Cyber TTP (Tactics Techniques and Procedures) issues within all types of specific sub-organisations: in particular, what does the decision-maker at this level need to know about when designing operational procedures, or similar?

601 Cyber Diplomacy & Internet Governance, Critical Infrastructure & Crisis Management, Intelligence & Counter-Intelligence, Military Cyber, Counter Cyber Crime – plus a number of 'cross mandate' activities including information exchange, research & education, and coordination.

organisations) at which stages. Different countries will emphasise different NCS mandates and cross-mandates according to their specific national preferences.

2. **The importance of different stakeholder groups (the 'Three Dimensions'):** probably no other subject in security policy has such a plethora of actors as does NCS. In fact, government is only one of the actor groups to consider. The other actors, namely the non-state 'societal' or 'national' actors as well as the international and transnational groups, are at least as important to any individual country's NCS as the government is. However, most liberal democratic governments have major conceptual challenges in engaging with these stakeholders. As shown in detail in Section 3, the challenge is to apply the lessons learned in other parts of security policy (such as peacekeeping or stabilisation operations) and apply them via public policy theory to NCS.

3. **Balancing the cost and benefits of security (the 'Five Dilemmas'):** the authors do not conceive of cyber security as being a zero-sum game. Ultimately, better cyber security should make a society both more prosperous and more free. However, in the short-term, NCS can have its costs, commensurate with the level of specific protection that is aimed for. As Section 1 explores in detail,[602] the policy challenge is to find the balance between economic growth and individual freedoms on the one hand and NCS requirements on the other. This balance is precarious. Overemphasising one side could ultimately be detrimental to both individual freedom and national security.

One advantage of this framework versus a more specific step-by-step approach is its universal application; not only to different types of democratic governmental systems, but also across different levels of technological sophistication and economic development. One of the most obvious realities is that there is a true global 'digital divide' – most NCS efforts are concentrated in highly developed economies, with a high reliance on information and communication technology (ICT). Most countries in the world have not, as of yet, developed a NCSS – often perceiving the risks associated with ICT as a 'rich world problem', and a relative minor one given the host of other concerns less developed nations have to deal with. This view is incorrect, for a number of reasons. Firstly, the economic development of all nations will increasingly be tied to issues relating to the stability of basic infrastructure,[603] and

---

602 These dilemmas are: (1) stimulate the economy vs. improve national security, (2) infrastructure modernisation vs. critical infrastructure protection, (3) private sector vs. public sector, (4) data protection vs. information sharing, (5) freedom of expression vs. political stability.

603 For an example of the importance of infrastructure development in China's development, see Pravakar Sahoo, Ranjan Kumar Dash, and Geethanjali Nataraj, Infrastructure Development and Economic Growth in China (Discussion Paper No. 261), (Chiba: Institute of Developing Economies, 2010), http://www.ide.go.jp/English/Publish/Download/Dp/pdf/261.pdf.

these infrastructures will increasingly be reliant upon ICT. Secondly, ICT is having a specific and direct impact on all aspects of economic and social development – from education to quality of life – and the advantages that accrue through this 'ICT for development'[604] approach will be imperilled if a government does not take appropriate measures to safeguard trust in the infrastructure. Finally, and by no means least importantly, the direct national security implications of the rise of ICT are universal. From new challenges to internal security to the threat of state-to-state conflict being carried out by 'cyber' means, all countries are impacted by this development, albeit to varying degrees.

## 6.2. FINAL REMARKS

The advent of the 'fifth domain' – the rise of cyberspace as a field of human endeavour – is probably nothing less than one of the most significant developments in world history. Cyberspace directly impacts every facet of human existence including economic, social, cultural and political developments, and the rate of change is not likely to stop anytime soon. Socio-political answers to the questions posed by the rise of cyberspace on the whole significantly lag behind the rate of technological change. Personal data, for instance, will remain a decisive issue for the foreseeable future, and one where the questions asked will depend on the specific ICT-enabled socio-economic developments. Who, for instance, could have predicted the role that social networks would be set to attain six, seven years ago? The rise of cyberspace means that as soon as one question is supposedly answered, many more appear – perhaps even invalidating the original question along the way.

The issue of NCS – both in its constituent components, but also as a subject or concept in its own right – is emblematic for the perpetual threat of obsolescence that stalks all attempts to adapt existing paradigms to this new world. A more extreme view could even state that the concept of 'national cyber security' is really nothing more than three illusions for the price of one: not only is cyberspace a faulty concept in its own right, it cannot be regulated in a national context and, at least in its present form, is inherently and perpetually insecure. Even a slightly more generous assessment of the validity of talking about cyber security in a national context could say that NCS is an insufficient construct. In the future, NCS will ultimately become a mainstreamed issue – something that will be included in all facets of public life more or less automatically, and will have no further validity than the term 'quality assurance' does today for all manufactured goods and processed

604 For an early example see Kerry McNamara, Poverty and Development: Learning from Experience, (Washington, DC: World Bank, 2003), http://www.infodev.org/en/Document.17.html.

foodstuffs. Talking about NCS is therefore akin to talking about 'national hygiene' – it depends on many factors that governments can only partially influence.

The concept of NCS introduced here is not intended to provide a strategic road-map that can be applied, in cookie-cutter fashion, to all government systems, in all perpetuity. Rather, it is an attempt to inform the reader on the comprehensive challenges that 'cyber' means for the security systems of the modern state, and how these challenges can be conceived of, and addressed, at different levels of government. Individual threats, strategic concepts, legislative frameworks and organisational structures will certainly change in the future – but the basic conceptual challenge to government will remain. As such, the very notion of 'national cyber security' may well be wrong. But for the time being, at least, it may prove useful.

Alexander Klimburg
Vienna, Austria
September 2012

# ANNEX: LIST OF PRINCIPAL GUIDELINES

## STARTING THE NATIONAL CYBER SECURITY STRATEGY

- **Importance:** every strategy starts with an acknowledgement of the importance of cyberspace and the rewards of a digital society, while stressing the precarious balance between cyber benefits and cyber risks (or threats). See Section 1.4.2 for more.
- **Threats:** a national cyber security strategy (NCSS) will typically include a section on threats, including terrorists, foreign nations, espionage, organise crime, or political activism. See Section 2.2.1 for more.
- **Definitions:** strategies often will also define important terms; however, exact definitions can be less important than descriptions and clarity in meaning. Not all NCSS use the same definitions; for example, some equate 'cyberspace' to essentially just the internet, while others embrace a far broader definition. See Section 1.2 for more.
- **Goal:** as with any national strategy, a NCSS should enable government departments to translate the vision into coherent and implementable policies; clarify how the nation might act in international affairs; and be linked to other, related strategies. See Section 2.1.1 for more.

## SCOPING THE NATIONAL CYBER SECURITY STRATEGY

A far-reaching NCSS will address all types (or 'mandates') of NCS. These have to equally be dealt with in the three areas (or 'dimensions') of state behaviour. However, a strategy that wanted to start small might focus on just a smaller subset, but would acknowledge the other mandates or dimensions.

**Three Dimensions.** A NCSS almost always focuses most on governmental activities, but should at least also mention international and national stakeholders as well. In future, these last two are likely to grow in importance as the role of international and non-state actors is increasingly realised. See Section 1.4.1 and Section 3.5 for more.

1. **Governmental:** requires a Whole of Government approach for improving the coordination of government actors.

2. **International:** a Whole of System approach for improving international, trans-border, and 'like-for-like' coordination.
3. **National:** a Whole of Nation approach for cooperating with internal national non-state actors, from civil society to critical infrastructure providers.

**Five Mandates.** Just as all NCSS must look across the three dimensions of governmental, international, and national actions, they should also consider the five main 'mandates' of governments in cyberspace. The most comprehensive strategies will include political aims, strategic goals and organisations for all five. See Section 1.4.2 and Section 4.5 for more.

1. **Military Cyber:** a national military must not only defend itself from cyber incidents but consider how to use cyber capabilities offensively as well. Defence is usually considered the first priority; however offensive capabilities will increasingly important in the future.
2. **Counter Cyber Crime:** fighting crime and reducing its impact are typical centrepieces for most NCSS.
3. **Intelligence and Counter-Intelligence:** using cyberspace for espionage – and stopping adversaries from doing the same – is increasingly important for states.
4. **Critical Infrastructure Protection and National Crisis Management:** includes protecting key sectors and institutional structures to enhance cooperation and response.
5. **Cyber Diplomacy and Internet Governance:** diplomacy adapting to the new global information environment, and managing the future of the internet.

There are also '**Cross Mandate**' areas including cyber security research and development, coordination, and information sharing and data protection.

**Five Dilemmas:** NCSS have to make implicit or explicit decisions about several key areas that can be seen as trade-offs between two public goods. See Section 1.5 for more.

1. **Stimulate the Economy or Improve National Security:** there can be an inherent tension between the openness required for innovation and the requirements of public security.
2. **Infrastructure Modernisation or Critical Infrastructure Protection:** the economic gains of adopting new technologies must be balanced against possible increases in security risks.
3. **Focus on Private Sector or Public Sector:** governments have a key role to play in cyber security but need to decide on either a 'regulatory' (mandated) or 'voluntary' approach to critical infrastructure protection.

4. **Data Protection or Information Sharing:** while information sharing is absolutely essential to NCS, the reality of (vitally needed) data protection legislation complicates these efforts.
5. **Freedom of Expression or Political Stability:** governments must ascertain to what extent, if any, they think the curtailment of 'internet freedoms' is justifiable for public safety.

**Common Themes:** The most common themes addressed in NCSS (and reflected in the frameworks above) are the following. See Section 2.2.1 for more.

- Maintaining a secure, resilient and trusted electronic operating environment,
- Promoting economic and social prosperity,
- Promoting trust and enabling business and economic growth,
- Overcoming the risk of information and communication technologies,
- Strengthening the resilience of infrastructures.

## NCSS DEVELOPMENT PROCESS

**Transparency and Coordination:** NCSS generally require more govermental coordination and public transparency than other strategies, as cyberspace does not belong to any department, or indeed any nation. Indeed, compared to other top-down national security issues, cyberspace is dominated by the bottom-up companies, non-state groups and citizens that build the networks and add content. Accordingly, each of the following issues has a special role to play, depending on the goals of the NCSS:

- **Tension between Military and Civilian, Law Enforcement and Intelligence:** because of fundamentally different approaches, each of these groups will want to influence the NCSS to favour their mandate. See Section 3.3 for more.
- **Transparency:** while many NCSS are unclassified, others are fully or partially classified. The more open the NCSS, the wider the goals of the nation acted upon by stakeholders during creation and implementation. This comes at the price of reducing 'strategic ambiguity' and can curtail a goverment's freedom of action. See Section 2.3 for more.
- **Coordination:** the importance of coordinating government activities across the various mandates cannot be overemphasised. In the very least, there must be a political policy coordination, but a strategic coordination body is helpful as well. See Section 4.6.1.
- **Development Process:** the development of a NCSS can occur primarily

top-down or bottom-up (i.e. building on existing expertise). Optimally, both processes need to occur at the same time. Similarly, governments can decide to draft a NCSS in a 'closed group' or larger 'big tent' approach, but should not attempt a 'reiterative' approach until a certain experience with the NCSS process exist.

### Balancing Offense and Defence

- Depending on their level of ambition, states will aim to protect their own government systems, assist in protecting the critical infrastructure, or extend to projecting power via cyberspace and cyberspace-related issues. Each of these levels of ambition will imply a slightly different stance; however these levels are not necessarily tied to a nation's respective size.
- A key aspect of both offensive and defensive stances in cyberspace is that both tasks will be accomplished by state and non-state actors, in both cases operating nationally and internationally. The greatly diverging institutional 'size' is however a poor indication of relevance – some of the most relevant actors will appear to be the least institutionalised. See Section 3.1.1 for more.
- Overall, the two most prevalent approaches to NCS can be described as 'deterrence' (imposing unacceptable costs to the attackers) or 'resilience' (denying the benefit to the attackers). Most nations will seek a balance of the two approaches depending on their ultimate level of ambition. See Section 3.2 for more.

## ORGANISING FROM THE STRATEGY

**Within Nations:** each of the five mandates has fundamentally different tasks and outlooks, and requires specific organisations. The cross-mandates help tied the disparate mandates together into a coherent NCS. See Sections 4.5, 4.6 and 4.7 for more.

1. **Military Cyber:** military cyber ranges from simply protecting the specific ICT systems (cyber defence) to enabling network-centric capabilities, supporting operational tasks, and accomplishing strategic missions.
2. **Counter Cyber Crime:** counter cyber crime activities will primarily involve organisations to facilitate law enforcement (such as public points of contact, forensic capabilities, etc.) as well as judicial means to facilitate prosecution. In some national cases these capabilities can largely lie outside of central-government control.
3. **Intelligence and Counter-Intelligence:** a primary beneficiary of many

cyber-related tasks, they will often seek to exploit cyber-means to facilitate information collection. At the same time they will depend on other collection capabilities (e.g., SIGINT) and international cooperation in order to be able to generate strategic intelligence on likely and actual cyber-adversaries.

4. **Critical Infrastructure Protection and National Crisis Management:** while CIP programmes are essentially preventative and crisis management essentially reactive, both aspects will largely depend upon Public-Private Partnerships (PPP) to generate intelligence and agree upon defensive and crisis management measures.
5. **Cyber Diplomacy and Internet Governance:** often dealt with in a highly disparate fashion (two largely contrasting world-views), it is necessary to connect both of these relevant aspects to be able to adequately represent a government position in the respective multilateral and bilateral frameworks.

**International:** national cyber security is never 'purely national'. The necessity of cooperation with a wide variety of international state and non-state actors needs to be appreciated in its complexity. These include government-to-government, international organisations, and non-state groups.

## OTHER ISSUES

**Aligned with Legal Commitments:** NCSS must also match international legal commitments. See Section 5.2 for more.

- Legal: UN Charter, International Court of Justice, International Telecommunications Union, prevention of terrorism and others,
- Cyber crime: Council of Europe Convention on Cybercrime,
- Human rights: Universal Declaration on Human Rights, European Convention on Human Rights,
- Military: International Humanitarian Law.

**Comply with Information Assurance Practices:** Information assurance practices are essential in any operational NCS.

- A NCSS must first and foremost tie to INFOSEC fundamentals, such as those defined in international standard 27002. See Section 5.3 for more. It is not necessary to have a single Information Security Management System (ISMS) across the entire government structure, but it is important that these different ISMS are interlocking.

**Aware of the NATO Cyber Dimension:** There are several issues that a NATO and a non-NATO nation might consider:

- Collective defence and cyber defence,
- Cooperation with non-NATO partners,
- NATO-EU Cooperation.

## LESSONS IDENTIFIED IN THE NCSS PROCESS

A review of other NCSS has revealed a number of important lessons identified:

- Resist making the document a 'one size fits all' by copying directly from other nation's strategies (Section 2.4),
- Link the NCSS to other national and international strategies (Section 2.4),
- Include a policy update and review mechanism (Section 2.4),
- Ensure there is both a top and mid-level interagency coordination group (Section 2.4),
- Identify critical services and infrastructure (Section 2.4),
- Create awareness, especially among policy-makers (Section 2.4),
- Don't underestimate the importance of 'talk' (exchange) (Section 3.6),
- Don't overestimate the importance of definitions (Section 3.6),
- Don't encourage path dependency (allowing essential strategic decisions to be made with a narrow and low-level framework) (Section 3.6),
- Encourage organisational flexibility (Section 3.6),
- Don't leave a policy vacuum (Section 4.8),
- Prevent organisational stovepipes (Section 4.8),
- Don't draft or accept obsolete legislation (Section 4.8),
- Enable flexible coordination (matrix structure) across operational components (Section 4.8),
- Clarify information exchanges and data protection issues (Section 4.8),
- Combat cyber illiteracy (Section 4.8),
- Neither under nor overvalue international commitments (Section 5.6),

- Integrate fundamental INFOSEC requirements (Section 5.6),
- Design around international interoperability (Section 5.6),
- Seek to learn from lessons identified (Section 5.6).

# BIBLIOGRAPHY

Additional Plenipotentiary Conference. *Constitution and Convention of the International Telecommunication Union*. Geneva: ITU, 1992.

———. *Instruments Amending the Constitution and Convention of the International Telecommunication Union (Geneva, 1992), Decisions, Resolutions and Recommendations*. Geneva: ITU, 1994.

AIV/CAVV. *Cyber Warfare*. The Hague: AIV, 2011. http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf.

Anderson, Mike. 'Trojans, Malware and Botnets got you down...?' *United States European Command*, 24 January 2012.

Andrues, Wesley R. 'What U.S. Cyber Command Must Do.' *Joint Forces Quarterly* 4, no. 59 (2010): 115-20.

Apps, Peter. 'Analysis: UK social media controls point to wider 'info war'.' *Reuters*, 18 August 2011.

Arveson, Paul. 'The Deming Cycle.' Balanced Scorecard Institute, http://www.balancedscorecard.org/TheDemingCycle/tabid/112/Default.aspx.

AS/NZS ISO 9000:2006. 'Quality management systems – fundamentals and vocabulary.'

Ashford, Warwick. 'BT extends cyber security agreement with MoD.' *ComputerWeekly.com*, 4 July 2012.

Assante, Michael. *Critical Cyber Asset Identification [Letter to Industry Stakeholders]*. Princeton, NJ: NERC, 2009. http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf.

Austin, Greg. 'China's Cybersecurity and Pre-emptive Cyber War.' *NewEurope*, 14 March 2011.

Australian Attorney-General's Department. *Cyber Security Strategy*. Canberra: Australian Government, 2009.

Australian Department of Foreign Affairs and Trade. *In the National Interest. Australia's Foreign and Trade Policy White Paper*. Canberra: Australian Department of Foreign Affairs and Trade, 1997.

Australian Government. 'Cyber Security Policy and Coordination Branch.'http://www.ag.gov.au/Organisationalstructure/Pages/CyberSecurityPolicyandCoordinationBranch.aspx.

Australian Prime Minister. *The First National Security Statement to the Australian Parliament*. Canberra: Australian Government, 2008.

Austrian Federal Chancellery. *National ICT Security Strategy Austria*. Vienna: Digital Austria, 2012.

Baer, Walter S., *et al. Machiavelli Confronts 21st Century Digital Technology: Democracy in a Network Society (Working Paper)*. Oxford: Oxford Internet Institute, 2009. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1521222.

Baker, Stewart, Shaun Waterman, and George Ivanov. *In the Crossfire. Critical Infrastructure in the Age of Cyber War*. Santa Clara, CA: McAfee, 2010. http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf.

Banusiewicz, John D. 'Lynn Outlines New Cybersecurity Effort.' *American Forces Press Service*, 16 June 2011.

Barno, David W. 'Challenges in Fighting a Global Insurgency.' *Parameters* 36, no. 2 (2006): 15-29.

Bartell, Frederick, *et al. Collaborating with the Private Sector*. Washington, DC: Global Innovation and Strategy Center, 2009. http://lsgs.georgetown.edu/programs/CyberProject/STRATCOM%20Report.pdf.

BBC. 'England riots: Twitter and Facebook users plan clean-up.' *BBC News*, 9 August 2011.

———. 'UK infrastructure faces cyber threat, says GCHQ chief.' *BBC News*, 12 October 2010.

Beardsley, Scott C., *et al.* 'Fostering the Economic and Social Benefits of ICT.' In *The Global Information Technology Report 2009-2010,* edited Soumitra Dutta and Irene Mia Geneva: World Economic Forum, 2010. http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf.

Beary, Brian. 'As momentum for action builds, EU's role remains unclear.' *Europolitics*, 3 May 2012.

Bellovin, Steven M., *et al.* 'Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure.' *Harvard National Security Journal* 3, no. 1 (2011): 1-38.

Biermann, Kai. 'CCC enttarnt Bundestrojaner.' *Die Zeit*, 8 October 2011.

Booz & Company. *Comparison and Aggregation of National Approaches (JLS/2008/D1/019 – WP 4)*. 2009.

Bradsher, Keith. 'China Asks Other Nations Not to Release Its Air Data.' *New York Times*, 5 June 2012.

Brauch, Hans G., *et al. Security and Environment in the Mediterranean: Conceptualising Security and Environmental Conflicts*. Berlin et al.: Springer Verlag, 2003.

Brennan, John O. 'Time to protect against dangers of cyberattack.' *The Washington Post*, 16 April 2012.

Brodie, Bernard. 'The Anatomy of Deterrence.' *World Politics* 11, no. 2 (1959): 173-91.

Bruce, Robert, *et al. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues (TNO Report 33680)*.

Delft: Tuck School of Business at Dartmouth, 2005. http://www.ists.dartmouth.edu/library/158.pdf.

Bull, Hedley. *The Anarchical Society: A Study of Order in World Politics*. Basingstoke: Macmillan, 1977.

Buzan, Barry, and Lene Hansen. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press, 2009.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security. A New Framework For Analysis*. London: Lynne Rienner Publishers, Inc., 1998.

Canadian Department for Public Safety. *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada*. Ottawa: Canadian Government, 2010.

Canadian Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. Ottawa: Canadian Government, 2004.

Canadian Security Intelligence Review Committee. *Checks and Balances. Viewing Security Intelligence Through the Lens of Accountability*. Ottawa: Canadian Security Intelligence Review Committee, 2011. http://www.sirc-csars.gc.ca/pdfs/ar_2010-2011-eng.pdf.

Carnegie Mellon University. 'About Us.' CERT, http://www.cert.org/meet_cert.

International Court of Justice. *Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium)*. ICJ Reports 2002, 3.

CDT. 'Chapter Three: Existing Privacy Protections.' In *CDT's Guide to Online Privacy*, edited by CDT. Washington, DC: CDT, 2009. https://www.cdt.org/privacy/guide.

Chaos Computer Club. 'Chaos Computer Club analyzes government malware.' CCC, http://ccc.de/en/updates/2011/staatstrojaner.

———. 'Chaos Computer Club leistet digitale Entwicklungshilfe für die Enquête-Kommission.' CCC, http://www.ccc.de/de/updates/2011/adhocracy-enquete.

Chapman, Glenn. 'Too Much Hysteria Over Cyber Attacks.' *Discovery News*, 16 February 2011.

Cheek, Michael W. 'What is Cyber War Anyway? A Conversation with Jeff Carr, Author of 'Inside Cyber Warfare'.' *The new new Internet*, 2 March 2010.

Chinese Information Office of the State Council. *The Internet in China (White Paper)*. Beijing: Government of the People's Republic of China, 2010.

Clausewitz, Carl von. *On War*. London: Penguin Books, 1982 [1832].

Clemente, Dave. *Defence and Cyber-security*. London: UK Parliament, 2012. http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs02.htm.

Clinton, Hillary R. 'Internet Freedom [Speech at Newseum in Washington, DC].' *Foreign Policy*,

21 January 2010.

comScore. 'It's a Social World: Top 10 Need-to-Knows About Social Networking and Where It's Headed. 'http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/it_is_a_social_world_top_10_need-to-knows_about_social_networking.

Conficker Working Group. 'Announcement of Working Group.' Conficker Working Group, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/FAQ#toc6.

Conger, Cristen. 'Could a single hacker crash a country's network?' http://computer.howstuffworks.com/hacker-crash-country-network1.htm.

Coram-James, Edward, and Tom Skinner. 'Most Amazing Internet Statistics 2012.' Funny Chunk, http://www.funnyjunk.com/channel/science/Most+Amazing+Internet+Statistics+2012/umiNGhz/.

Council of the European Union. *Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA)*. Official Journal of the European Union, L 121.

Council of the European Union. *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*. Official Journal of the European Union, L 69.

Council of the European Union. *Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*. Official Journal of the European Union, L 330.

Council of the European Union. *Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)*. Official Journal of the European Union, L 164.

Council of Europe. *Convention on Cybercrime (ETS No. 185)*. Budapest: Council of Europe, 2001.

———. 'Convention on Cybercrime (Treaty Status).' http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

———. *Council of Europe Explanatory Report to the Convention on Cybercrime (ETS No. 185)*. Strasbourg: Council of Europe, 2001. http://conventions.coe.int/Treaty/EN/Reports/html/185.htm.

———. *Declaration by the Committee of Ministers on Internet governance principles*. Strasbourg: Council of Europe, 2011.

CPNI.NL. 'Werkwijze ISACs.' CPNI.NL, https://www.cpni.nl/informatieknooppunt/werkwijze-isacs.

Cyber. Merriam-Webster, http://www.merriam-webster.com/dictionary/cyber.

Czech Ministry of Interior. *Czech Cyber Security Strategy for the Period 2011–2015*. Prague: ENISA, 2011.

Dale, Catherine. *National Security Strategy: Legislative Mandates, Execution to Date, and Considerations for Congress*. Washington, DC: Congressional Research Service, 2008. http://fpc.state.gov/documents/organization/106170.pdf.

Dean, David, *et al.* 'The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy.' *BCG. Perspectives*, 27 January 2012.

Defense System Staff. 'Overlapping defense essential to deter cyberattacks: Panel members.' *Defense Systems*, 8 November 2011.

Denef, Sebastian, *et al. ICT Trends in European Policing*. Sankt Augustin: Fraunhofer-Institut für Angewandte Informationstechnik FIT, 2011. http://www.fit.fraunhofer.de/content/dam/fit/de/documents/composite_d41.pdf.

Deterrence. *Oxford English Dictionary Online*. Oxford University Press, 2012.

Detica. *The Cost of Cyber Crime. A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*. London: UK Cabinet Office, 2011. http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf.

European Parliament and the Council. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Official Journal, L 281.

European Parliament and the Council. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Official Journal, L 201.

Directorate General for Internal Policies. *Briefing Note: Digital Agenda for Europe – An Overview for the 37th EEA JPC*. Strasbourg: European Parliament, 2011. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/deea/dv/1011_10_/1011_10_en.pdf.

Dowdy, John. 'The Cybersecurity Threat to U.S. Growth and Prosperity.' In *Securing Cyberspace: A New Domain for National Security*, edited by Nicholas Burns and Jonathon Price. Washington, DC: Brookings Institution Press, 2012.

International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. Report of the International Law Commission. Fifty-third session 2001, Supplement No. 10 (A/56/10).

Dutch Government. *Strategie Nationale Veiligheid*. The Hague: Ministry of the Interior and Kingdom Relations, 2007.

Dutch Ministry of Housing, Spatial Planning, and the Environment. *Handreiking Security Management*. The Hague: Dutch Ministry of Housing, Spatial Planning and the Environment, 2008. http://www.rijksoverheid.nl/bestanden/documenten-en-

publicaties/brochures/2010/11/26/handreiking-security-management/11br2008g225-2008613-154851.pdf.

Dutch Ministry of Security and Justice. 'The National Cyber Security Strategy (NCSS). Strength through Cooperation.' The Hague: National Coordinator for Counterterrorism and Security, 2011.

———. 'The National Cyber Security Strategy. Strength Through Cooperation.' The Hague: Dutch Ministry of Security and Justice, 2011.

Dutta, Soumitra, and Irene Mia. *The Global Information Technology Report 2009-2010. ICT for Sustainability*. Geneva: World Economic Forum, 2010. http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf.

EastWest Institute. *International Pathways to Cybersecurity. Report of Consultation*. Brussels: EastWest Institute, 2010. http://www.ewi.info/system/files/CyberSummaryReport.pdf.

Eijndhoven, Don. 'Dutch Cyber Security Council Now Operational.' *Infosec Island*, 5 July 2011.

Eitzen, Christopher von. 'Online attacks on Swiss foreign ministry.' *The H Security*, 27 October 2009.

English.news.cn. 'China, ROK, Japan pledge future-oriented partnership amid trilateral summit: joint declaration.' *English.news.cn*, 14 May 2012.

ENISA. 'CERT Inventory.' ENISA, http://www.enisa.europa.eu/activities/cert/background/inv.

———. *National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace*. Heraklion: ENISA, 2012. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport.

Espiner, Tom. 'US cyber-tsar: Tackle jailbroken iPhones.' *ZDNet*, 24 March 2012.

Espionage. Merriam-Webster, http://www.merriam-webster.com/dictionary/espionage.

Estonian Ministry of Defence. *Cyber Security Strategy*. Tallinn: Estonian Ministry of Defence, 2008.

Estonian Ministry of Foreign Affairs. 'Around 150 Experts Associated with Estonia's Cyber Defence League.' *Estonian Review*, 3 October 2011.

EU-NATO. *The Framework for Permanent Relations and Berlin Plus*. Brussels: Council of the European Union, 2003.

European Commission. *Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM(2012) 140 final)*. Brussels: European Commission, 2012.

———. *Towards a general policy on the fight against cyber crime (COM(2007) 267 final)*. Brussels: European Commission, 2007.

European Union. 'Critical infrastructure protection.' http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm.

———. *Treaty on European Union ('Treaty of Maastricht')*. Brussels: Official Journal C 191, 1992.

*European Union Guidelines on promoting compliance with international humanitarian law (IHL)*. 2009/C 303/06.

Europol. 'European Cybercrime Centre to be Established at Europol.' *Media Corner*, 28 March 2012.

———. *Threat Assessment (Abridged). Internet Facilitated Organised Crime (iOCTA)*. The Hague: Europol, 2011. https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf.

Evans, Dave. *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*. San Jose, CA: Cisco Internet Business Solutions Group, 2011. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Federal Ministry of Defence. *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*. Berlin: Federal Ministry of Defence, 2006.

FIRST. 'Best Practices Contest 2008: Project.' http://www.first.org/conference/2008/contest.html.

———. 'FIRST Vision and Mission Statement.' FIRST, http://www.first.org/about/mission.

Forestier, Anthony M. 'Effects-Based Operations: An Underpinning Philosophy for Australia's External Security?'. *Security Challenges* 2, no. 1 (2006).

Foucault, Michel. *'Society must be defended': Lectures at the Collège de France, 1975-1976*. New York: Pan Books Limited, 2003.

French Secretariat-General for National Defence and Security. *Information systems defence and security. France's strategy*. Paris: French Network and Information Security Agency, 2011.

French White Paper Commission. *The French White Paper on Defence and National Security*. Paris: Odile Jacob, 2008.

Frontier Economics Europe. *Estimating the global economic and social impacts of counterfeiting and piracy. A Report commissioned by Business Action to counterfeiting and piracy (BASCAP)*. Paris: ICCWBO, 2011. http://www.iccwbo.org/Data/Documents/Bascap/Global-Impacts-Study---Full-Report.

Gabriëlse, Robbert. 'A 3D Approach to Security and Development.' *PfP Consortium Quarterly Journal* 6, no. 2 (2007): 67-73.

GAO. *Defense Department Cyber Efforts. More Detailed Guidance Nedded to Ensure Military Services Develop Appropriate Cyberspace Capabilities*. Washington, DC: GAO, 2011.

http://www.gao.gov/products/GAO-11-421.

Gayathri, Amrutha. 'Iran To Shut Down Internet Permanently; 'Clean' National Intranet In Pipeline.' *International Business Times*, 9 April 2012.

Gercke, Marco. 'Regional and International Trends in Information Society Issues.' In *HIPCAR – Working Group 1*. St. Lucia: ITU, 2010.

German Federal Ministry of the Interior. *Cyber-Sicherheitsstrategie für Deutschland*. Berlin: German Federal Ministry of the Interior, 2011.

———. *Cyber Security Strategy for Germany*. Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011.

———. *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen*. Berlin: German Federal Ministry of the Interior, 2007.

Gjelten, Tom. 'Stuxnet Raises 'Blowback' Risk In Cyberwar.' *npr*, 2 November 2011.

Goitein, Elizabeth, and David M. Shapiro. *Reducing Overclassification Through Accountability*. New York: Brennan Center for Justice, 2011. http://brennan.3cdn.net/3cb5dc88d210b8558b_38m6b0ag0.pdf.

Goldsmith, Jack, and Melissa Hathaway. 'The cybersecurity changes we need.' *The Washington Post*, 29 May 2010.

Gorman, Siobhan, and Julian E. Barnes. 'Cyber Combat: Act of War.' *The Wall Street Journal*, 30 May 2011.

Government of the Netherlands. 'Crisis response organisation operated effectively during DigiNotar crisis.' *News item*, 28 June 2012.

Grauman, Brigid. *Cyber-security: The vexed question of global rules. An independent report on cyber-preparedness around the world*. Brussels: Geert Cami, 2012. http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf.

Greene, Jamal. 'Hate Speech and the Demos.' In *The Content and Context of Hate Speech: Rethinking Regulation and Responses*, edited by Michael Herz and Péter Molnár. Cambridge et al.: Cambridge University Press, 2012.

Group of Governmental Experts. *Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)*. New York: United Nations, 2011. http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf.

Haas, Marcel de. *From Defence Doctrine to National Security Strategy: The Case of the Netherlands*. The Hague: Netherlands Institute of International Relations Clingendael, 2007. http://www.clingendael.nl/publications/2007/20071100_cscp_art_srsa_haas.pdf.

Hale, Julian. 'NATO Official: Cyber Attack Systems Proliferating.' *DefenceNews*, 23 March

2010.

Hallingstad, Geir, and Luc Dandurand. *Cyber Defence Capability Framework – Revision 2. Reference Document RD-3060*. The Hague: NATO C3 Agency, 2010.

Harley, Brian. 'A Global Convention on Cybercrime?' *Science and Technology Law Review*, 23 March 2010.

Hathaway, Melissa. 'Power Hackers: The U.S. Smart Grid Is Shaping Up to Be Dangerously Insecure.' *Scientific American*, 5 October 2010.

Hathaway, Melissa E. 'Falling Prey to Cybercrime: Implications for Business and the Economy.' In *Securing Cyberspace: A New Domain for National Security*, edited by Nicholas Burns and Jonathon Price. 145-57. Queenstown, MD: Aspen Institute, 2012.

———. 'Leadership and Responsibility for Cybersecurity.' *Georgetown Journal of International Affairs* Special Issue (Forthcoming).

———. 'Toward a Closer Digital Alliance.' *SAIS Review* 30, no. 2 (2010): 21-31.

Hathaway, Melissa E., and John E. Savage. *Stewardship of Cyberspace. Duties for Internet Service Providers*. Cambridge, MA: Belfer Center for Science and International Affairs, 2012. http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012_hathaway-savage.pdf.

Healey, Jason. 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms.' *New Atlanticist*, 21 September 2011.

———. 'Bringing a Gun to a Knife Fight: US Declaratory Policy and Striking Back in Cyber Conflict.' *Atlantic Council Issue Brief*, September 2011.

Healey, Jason, and Leendert van Bochoven. 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.' *Atlantic Council Issue Brief*, February 2012.

Healey, Jason, *et al. Lessons From Our Cyber Past: The First Military Cyber Units [Transcript]*. Washington, DC: Atlantic Council, 2012. http://www.acus.org/event/lessons-our-cyber-past-first-military-cyber-units/transcript.

Healey, Jason, and Karl Grindal. 'Lessons from the First Cyber Commanders.' *New Atlanticist*, 14 March 2012.

Healey, Jason, *et al. Building a Secure Cyber Future: Attacks on Estonia, Five Years On [Transcript]*. Washington, DC: Atlantic Council, 2012. http://www.acus.org/event/building-secure-cyber-future-attacks-estonia-five-years/transcript.

Heickerö, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. Stockholm: Swedish Defence Research Agency 2010. http://www.highseclabs.com/Corporate/foir2970.pdf.

Holden, Michael. 'Cyber crime costs UK $43.5 billion a year: study.' *Reuters*, 17 February 2011.

Holling, Crawford S. 'Engineering Resilience versus Ecological Resilience.' In *Engineering Within Ecological Constraints*, edited by Peter C. Schulze. Washington, DC, 1996.

———. 'Resilience and Stability of Ecological Systems.' Vancouver: Institute of Resource Ecology, 1973.

Holman, Tyler. 'Anonymous threatens to bring down the internet.' *Neowin.net*, 27 March 2012.

Homeland Security News Wire. 'GAO: U.S. slow to implement president's cyber security strategy.' *Homeland Security News Wire*, 20 October 2010.

US Executive Office of the President. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7)*.

Hunan People's Publishing House. *China Cyber Warfare: We Can't Lose the Cyber War*. Hunan: China South Publishing & Media Group.

ICAO. *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation ('Montreal Convention') (974 UNTS 177)*. Montreal: International Conference on Air Law, 1971.

ICDRM. *Emergency Management Glossary of Terms*. Washington, DC: George Washington University, 2010. http://www.gwu.edu/~icdrm/publications/PDF/GLOSSARY%20-%20Emergency%20Management%20ICDRM%2030%20JUNE%2010.pdf.

ICRC. *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention)*. Geneva: ICRC, 1949.

ICS-CERT. *ICS-CERT Monthly Monitor*. Washington, DC: US Department of Homeland Security, 2012. http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf.

IETF RFC 2350. 'Expectations for Computer Security Incident Response.' June 1998, http://tools.ietf.org/html/rfc2350.

Ilves, Luukas. 'Cyber Security Trends and Challenges.' In *Cyber Security Trends and Challenges: Latvian and Estonian Perspective*. Riga: CERT.LV, 2012.

Immarsat. 'Legal notices. Terms and Conditions of Use. 'http://www.inmarsat.com/Terms_and_conditions.aspx.

Indian Ministry of Communications and Information Technology. *Discussion Draft on National Cyber Security Policy*. New Delhi: Government of India, 2011.

Institute, EastWest, and Moscow State University. *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations*. Brussels and Moscow: EastWest Institute and Moscow State University, 2011.

INTELSAT General Corporation. 'Terms of Use.' http://www.intelsatgeneral.com/terms.

International Court of Justice. 'The Court.' http://www.icj-cij.org/court/index.php?p1=1.

International Law Commission. 'United Nations', https://www.un.org/law/ilc.

INTERPOL. 'Cybercrime.' http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

———. 'INTERPOL and ICANN advance cooperation on Internet security after historic first meeting.' *Media Release*, 23 May 2011.

ISACA. *G41 Return on Security Investment (ROSI)*. Rolling Meadows, IL: ISACA, 2010. http://www.isaca.org/Knowledge-Center/Standards/Documents/G41-ROSI-5Feb10.pdf.

ISO/IEC 27001:2005. 'Information technology – Security techniques – Information security management systems – Requirements.'

ISO/IEC 27002:2005. 'Information technology – Security techniques – Code of practice for information security management.'

ISO/IEC 27032:2012. 'Information technology – Security techniques – Guidelines for cybersecurity.'

ISO/IEC TR 27008:2011. 'Information technology – Security techniques – Guidelines for auditors on information security controls.'

ITU-D. *The World in 2010. ICT Fact and Figures*. Geneva: ITU, 2010. http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

ITU. *ITU National Cybersecurity Strategy Guide*. Geneva: ITU, 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

———. *Measuring the Information Society*. Geneva: ITU, 2011. http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf.

Jandl, Gerhard. 'The Challenges of Cyber Security – a Government's Perspective.' *Human Security Perspectives*, no. 1 (2012): 26-37.

Japanese Information Security Policy Council. *Information Security Strategy for Protecting the Nation*. Tokyo: National Information Security Center, 2010.

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1976.

Klaver, Marieke, Eric Luiijf, and Albert Nieuwenhuijs. *The RECIPE Project: Good Practices Manual for CIP Policies. For Policy Makers in Europe*. Brussels: European Commission, 2011. http://www.tno.nl/recipereport.

Klimburg, Alexander. 'Gesamtstaatliche Ansätze zur Cybersicherheit. Erfahrungen aus Österreich.' In *Strategie und Sicherheit 2012. Der Gestaltungsspielraum der österreichischen Sicherheitspolitik*, edited by Johann Pucher and Johann Frank. 463-71. Wien et al.: Böhlau Verlag, 2012.

———. 'Lessons from the Comprehensive Approach for Whole of Nation Cybersecurity.' *Per Concordiam* 2, no. 2 (2011): 28-33.

———. 'Mobilising Cyber Power.' *Survival* 53, no. 1 (2011): 41-60.

———. 'Whole-of-Nation Cyber Security.' In *Inside Cyber Warfare*, edited by Jeffrey Carr. 199-202. Sebastopol, CA: O'Reilly Media, 2009.

———. 'The Whole of Nation in Cyberpower.' *Georgetown Journal of International Affairs* Special Issue (2011).

Klimburg, Alexander, and Philipp Mirtl. *Cyberspace and Governance – A Primer (Working Paper 65)*. Vienna: Austrian Institute for International Affairs, 2012. http://www.oiip.ac.at/publikationen/arbeitspapiere/publikationen-detail/article/92/cyberspace-and-governance-a-primer.html.

Klimburg, Alexander, and Heli Tirmaa-Klaar. *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*. Brussels: European Parliament, 2011. http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf.

Kramer, Franklin D., Stuart H. Starr, and Larry Wentz, eds. *Cyber Power and National Security*. Washington, DC: National Defence UP, 2009.

Kurbalija, Jovan. 'Is tweeting a breach of diplomatic function?' *DiploFoundation*, 14 June 2012.

International Court of Justice. *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*. ICJ Reports 1996, ICJ 226, para. 86.

Lewis, James. 'Confidence-building and international agreement in cybersecurity.' *Disarmament Forum*, no. 4 (2011): 51-59.

Lewis, James A., and Katrina Timlin. *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization*. Geneva: UNIDIR, 2011. http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

Libicki, Martin C. *Cyberdeterrance and Cyberwar*. Pittsburgh: RAND Corporation, 2009.

Lindell, Michael K., Carla S. Prater, and Ronald W. Perry. *Fundamentals of Emergency Management* Washington, DC: FEMA, 2006. http://training.fema.gov/EMIWeb/edu/fem.asp.

Lithuanian Government. *Resolution NO 796 on the Approval of the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019*. Vilnius: Information Technology and Communications Department, 2011.

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. 'Nineteen National Cyber Security Strategies.' *International Journal of Critical Infrastructures* (forthcoming).

Luiijf, Eric, *et al.* 'Ten National Cyber Security Strategies: a Comparison.' In *Critical Information Infrastructure Security*, edited by Bernhard M. Hämmerli and Stephen D. Wolthusen. Springer-Verlag, forthcoming.

Lupovici, Amir. 'The Emerging Fourth Wave of Deterrence Theory – Toward a New Research

Agenda.' *International Studies Quaterly* 54, no. 3 (2010): 705-32.

Luxembourg Government. *Stratégie nationale en matière de cyber sécurité*. Luxembourg: Government of the Grand Duchy of Luxembourg, 2011.

Mallery, John C. 'International Data Exchange And A Trustworthy Host: Focal Areas For International Collaboration In Research And Education.' In *Digital ecosystems network and information security and how international cooperation can provide mutual benefits*. Brussels: BIC, 2011.

———. 'Models of Escalation and Desescalation in Cyber Conflict.' In *Workshop on Cyber Security and Global Affairs* Budapest: International Cyber Center at GMU and CERT-Hungary, 2011.

Mari, Angelica. 'IT's Brazil: The National Broadband Plan' *itdecs.com*, 26 July 2011.

Maurer, Tim. *Cyber Norm Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-Security*. Cambridge, MA: Belfer Center for Science and International Affairs, 2011. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

McNamara, Kerry. *Poverty and Development: Learning from Experience*. Washington, DC: World Bank, 2003. http://www.infodev.org/en/Document.17.html.

Meisner, Jeffrey. 'Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets.' *The Official Microsoft Blog*, 25 March 2012.

Melvin, Jasmin. 'White House lobbies for cybersecurity bill amid worries it may stall.' *Reuters*, 1 August 2012.

Melzer, Nils. 'Cyber operations and *jus in bello*.' *Disarmament Forum*, no. 4 (2011): 3-17.

Meridian. 'The Meridian Process.' Meridian2007, http://www.meridian2007.org/.

Merrell, Sam, John Haller, and Philip Huff. *Public-Private Partnerships: Essential for National Cyber Security [Transcript]*. Pittsburgh, PA: Carnegie Mellon University, 2010. http://www.cert.org/podcast/show/20101130merrell.html.

International Court of Justice. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. ICJ Reports 1986, 70.

Miller, Jason. 'Agencies must use Cyberscope tool for FISMA reports.' *Federal News Radio*, 15 September 2011.

Ministry of Communications and Information Society. *Strategia de securitate cibernetică a României*. Bucharest: Ministry of Communications and Information Society, 2011.

Mosneagu, Bodgan, Edgardo Vasquez, and Jay Lam. 'Information Security as a Profession.' 2012.

Mudge, Raphael S., and Scott Lingley. 'Cyber and Air Joint Effects Demonstration (CAAJED).'

AFRL/RIGB, 2008.

Mullen, Michael G. 'Working Together: Modern Challenges Need 'Whole-of-Nation' Effort.' *JFQ* 4, no. 59 (2010): 2-3.

Napolitano, Janet. *State of America's Homeland Security Address [Remarks]*. Washington, DC: Department of Homeland Security, 27 January 2011. http://www.dhs.gov/news/2011/01/27/state-americas-homeland-security-address.

US Executive Office of the President. *National Security Presidential Directive 54: Cyber Security and Monitoring (NSPD-54) / Homeland Security Presidential Directive 23: Cyber Security and Monitoring (HSPD-23)*.

NATO. *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, adopted by Heads of State and Government at the NATO in Lisbon 19-20 November 2010*. Brussels: NATO Public Diplomacy Division, 2010. http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

———. *The Alliance's New Strategic Concept*. London: NATO, 1991.

———. *Chicago Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012*.Brussels: NATO, 2012. http://www.nato.int/cps/en/SID-D03EFAB6-46AC90F8/natolive/official_texts_87593.htm?selectedLocale=en.

———. 'Cyber defence: next steps.' *NATO Newsroom*, 10 June 2011.

———. *Defending the networks. The NATO Policy on Cyber Defence*.Brussels: NATO Public Diplomacy Division, 2011. http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

———. *Lisbon Summit Declaration*. Lisbon: NATO, 2010.

———. 'NATO-EU: a strategic partnership.' http://www.nato.int/cps/en/natolive/topics_49217.htm.

———. 'NATO and cyber defence.' http://www.nato.int/cps/en/SID-714ABCE0-30D8F09C/natolive/topics_78170.htm.

———. 'The NATO Defence Planning Process.' http://www.nato.int/cps/en/natolive/topics_49202.htm.

———. 'NATO Rapid Reaction Team to fight cyber attack.' *NATO Newsroom*, 13 March 2012.

———. 'The Science for Peace and Security Programme'. http://www.nato.int/cps/en/SID-51871B1B-CD538A0D/natolive/topics_85373.htm.

———. *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*. Lisbon: NATO, 2010.

Naughton, John. 'Thanks, Gutenberg – but we're too pressed for time to read.' *The Guardian*, 27 January 2008.

New Zealand Ministry of Economic Development. *New Zealand's Cyber Security Strategy*. Wellington: New Zealand Ministry of Economic Development, 2011.

NITRD. 'Interagency Working Group on Cyber Security and Information Assurance (CSIA IWG).' NITRD, https://connect.nitrd.gov/nitrdgroups/index.php?title=Interagency_Working_Group_on_Cyber_Security_and_Information_Assurance_%28CSIA_IWG%29.

Noshiravani, Reyhaneh. 'NATO and Cyber Security: Building on the Strategic Concept.' *Chatham House Rapporteur Report*, 20 May 2011.

NSA. *Defense In Depth. A practical strategy for achieving Information Assurance in today's highly networked environments*. USA. http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

Nye, Joseph S. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

———. *The Future of Power*. New York: PublicAffairs, 2011.

O'Hara, Colleen. 'Global Cyber Sleuth. The State Department's Chris Painter relishes his role as a cyber diplomat.' *Leadership* Winter (2012): 36-43.

O'Shea, Kevin. 'Cyber Attack Investigative Tools and Technologies.' In *HTCIA*. Hanover, NH: Dartmouth College, 2003.

OECD. *A Comprehensive Response to Conflict and Fragility*. Paris: OECD, 2009. http://www.oecd.org/development/conflictandfragility/44392383.pdf.

———. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD, 1980.

———. *Whole of Government Approaches to Fragile States*. Paris: OECD, 2006. http://www.oecd.org/dac/conflictandfragility/whole-of-governmentapproachestofragilestates.htm.

OIC-CERT. 'Mission Statement'. OIC-CERT, www.oic-cert.net.

Operation. *Oxford English Dictionary Online*. Oxford University Press, 2012.

Ortiz, Catherine. 'DOD Trusted Foundry Program: Ensuring 'Trust' for National Security & Defense Systems.' In *NDIA Systems Engineering Division Meeting*. Arlington, VA: Trusted Foundry Program, 2012.

OSCE. *The OSCE Concept of Comprehensive and Co-operative Security. An Overview of Major Milestones (SEC/CPC/OS/167/09)*. Vienna: OSCE, 2009.

Plenipotentiary Conference. *Constitution of the International Telecommunication Union (Geneva, 1992) as amended by subsequent plenipotentiary conferences*. Geneva: ITU, 2006.

Policy. *Oxford English Dictionary Online*. Oxford University Press, 2012.

Ponemon Institute. *2010 Annual Study: U.K. Cost of a Data Breach. Compliance pressures, cyber attacks targeting sensitive data drive leading IT organisations to sometimes pay more than necessary.* Mountain View, CA: Symantec Corporation, 2011. http://www.symantec.com/content/en/us/about/media/pdfs/UK_Ponemon_CODB_2010_031611.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach.

Potter, Evan H., ed. *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. Quebec: McGill-Queen's University Press, 2002.

Potter, Ned. '"Wikipedia Blackout,' SOPA and PIPA Explained.' *ABC News*, 17 January 2012.

Press Trust of India. 'PM-led National Security Council discusses cyber security.' *Daily News and Analysis*, 28 June 2012.

Prince, Brian. 'NSA: Assume Attackers Will Compromise Networks.' *eWeek.com*, 17 December 2010.

Pring, Cara. '100 Social Media, Mobile and Internet Statistics for 2012 (March).' *The Social Skinny*, 21 March 2012.

Public Safety and Emergency Preparedness Canada. *Ontario – U.S. Power Outage – Impacts on Critical Infrastructure*. Ottawa: Public Safety Canada, 2006. http://www.publicsafety.gc.ca/prg/em/_fl/ont-us-power-e.pdf.

Public Safety and Homeland Security Bureau. 'Tech Topic 20: Cyber Security and Communications.' FCC, http://transition.fcc.gov/pshs/techtopics/techtopics20.html.

Rademaker, Michel. 'National Security Strategy of the Netherlands: An Innovative Approach.' In, *Information and Security* 23, no. 1 (2008): 51-61. http://infosec.procon.bg/v23/Rademaker.pdf.

International Court of Justice. *Rainbow Warrior Case (New Zealand v. France). Ruling of the UN Secretary-General of 6 July 1986.* 74 ILR 241.

Rattray, Gregory, and Jason Healey. 'Categorizing and Understanding Offensive Cyber Capabilities and Their Use.' In *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy*, edited by National Research Council. 77-97. Washington, DC: The National Academies Press, 2010.

Reichl, Johannes, and Michael Schmidthaler. *Blackouts in Österreich Teil I – Analyse der Schadenskosten, Betroffenenstruktur und Wahrscheinlichkeiten großflächiger Stromausfälle*. Linz: Johannes Kepler Universität Linz, 2011. http://energyefficiency.at/web/projekte/blacko.html.

Reilly, Sean. 'IG Reviewing Overclassification at DoD.' *Defense News*, 8 February 2012.

Research Division. *Internet: case-law of the European Court of Human Rights*. Strasbourg:

European Court of Human Rights, 2011. http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_EN.pdf.

Reuters. 'South Korea discovers downside of high speed internet and real-name postings.' *The Guardian*, 6 December 2011.

Rid, Thomas. 'Cyber War Will Not Take Place.' *The Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

Rintakoski, Kristiina, and Mikko Autti. *Comprehensive Approach. Trends, Challenges and Possibilities for Cooperation in Crisis Prevention and Management*. Helsinki: Finish Ministry of Defence, 2008. http://www.defmin.fi/files/1316/Comprehensive_Approach_-_Trends_Challenges_and_Possibilities_for_Cooperation_in_Crisis_Prevention_and_Management.pdf.

Robert O'Harrow. 'Cyber search engine Shodan exposes industrial control systems to new risks.' *The Washington Post*, 3 June 2012.

Rodriguez, Chris. 'Vulnerability Bounty Hunters.' *Frost & Sullivan*, 3 February 2012.

Romani, Roger. *Rapport d'informations sur la cyberdéfense*. Paris: Sénat, 2008.

Sahoo, Pravakar, Ranjan Kumar Dash, and Geethanjali Nataraj. *Infrastructure Development and Economic Growth in China (Discussion Paper No. 261)*. Chiba: Institute of Developing Economies, 2010. http://www.ide.go.jp/English/Publish/Download/Dp/pdf/261.pdf.

SANS Institute. *An Introduction to TEMPEST*. Bethesda, ML: SANS Institute, 2012. http://www.sans.org/reading_room/whitepapers/privacy/introduction-tempest_981.

Schaffer, Greg. *Federal Information Security Memorandum. FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. edited by US Department of Homeland Security. Arlington, VA 2012.

Schmitt, Michael N. 'Cyber Operations and the Jus Ad Bellum Revisited.' In, *Villanova Law Review* 56, (2011): 569-605. http://www.usnwc.edu/getattachment/f1236094-416b-4e5b-bf58-32e677aed04a/villanova_cyber_ad_bellum.

———, gen. ed. Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, forthcoming 2013.

Schober, Marc. 'Aktuelles zu Kritischen Infrastrukturen.' In *SECMGT-Workshop*. DB Systel GmbH: Gesellschaft für Informatik, 2011.

Shalal-Esa, Andrea. 'Ex-U.S. general urges frank talk on cyber weapons.' *Reuters*, 6 November 2011.

Shanghai Cooperation Organization. *Agreement on Cooperation in the Field of Ensuring International Information Security [based on unofficial translation]*. Yekaterinburg:

Shanghai Cooperation Organization, 2009.

Sommer, Peter, and Ian Brown. *Reducing Systemic Cybersecurity Risk*. Paris: OECD, 2011. http://www.oecd.org/sti/futures/globalprospects/46889922.pdf.

South Africa Department of Communications. *Notice of Intention to Make South African National Cybersecurity Policy (Draft approved 11 March 2012)*. Pretoria: South Africa Government, 2010.

Spanish Government. *Spanish Security Strategy. Everyone's responsibility*. Madrid Spanish Government, 2011.

State Government Victoria. *Victorian approaches to joined up government. An overview*. Melbourne: State Services Authority, 2007. http://www.ssa.vic.gov.au/images/stories/product_files/71_joined_up_government.pdf.

Statistic Brain. 'Skype Statistics.' *Statistic Brain*, 28 March 2012.

Stavridis, James G., and Elton C. Parker. 'Sailing the Cyber Sea.' In, *JFQ* 2, no. 65 (2012): 61-7.

Strategy. *Oxford English Dictionary Online*. Oxford University Press, 2012.

Swaine, Jon. 'Georgia: Russia 'conducting cyber war'.' *The Telegraph*, 11 August 2008.

Swiss Federal Department of Defence, Civil Protection, and Sports. *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken*. Bern: Swiss Confederation, 2012.

Symantec Corporation. *Internet Security Threat Report: 2011 Trends*. Mountain View, CA: Symantec Corporation, 2012. http://www.symantec.com/threatreport.

Syntegra. 'Common Criteria. An Introduction.' NIAP, http://www.niap-ccevs.org/cc-scheme/cc_docs/cc_introduction-v2.pdf.

Tactical. *Oxford English Dictionary Online*. Oxford University Press, 2012.

Tehan, Rita. *Cybersecurity: Authoritative Reports and Resources*. Washington, DC: Congressional Research Service, 2012. http://www.fas.org/sgp/crs/misc/R42507.pdf.

US House of Representatives. *Testimony: Before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives: Committee on Homeland Security*, 28 June 2012.

The Dutch Safety Board. http://www.onderzoeksraad.nl/en.

———. *The DigiNotar Incident: Why digital safety fails to attract enough attention from public administration*. The Hague: Dutch Safety Board, 2012. http://www.onderzoeksraad.nl/docs/rapporten/Rapport_Diginotar_EN_summary.pdf.

The Economist. 'The Growing Appeal of Zero. Banning the bomb will be hard, but not impossible.' *The Economist*, 16 June 2011.

The Rendon Group. *Conficker Working Group: Lessons Learned*. Washington, DC: Conficker Working Group, 2011. http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

Thompson, Mark. 'U.S. Cyberwar Strategy: The Pentagon Plans to Attack.' *Time*, 2 February 2010.

TNN. 'India and Japan agree to boost maritime, cyber security.' *The Times of India*, 1 May 2012.

Uganda Ministry of Information and Communications Technology. *National Information Security Strategy (NISS Final Draft)*. Kampala: Uganda Ministry of Information and Communications Technology, 2011.

UK Cabinet Office. *Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space*. Norwich: The Stationery Office, 2009.

———. *The National Security Strategy of the United Kingdom. Security in an interdependent world*. Norwich: The Stationery Office, 2008.

———. *The National Security Strategy of the United Kingdom: Update 2009. Security for the Next Generation*. Norwich: The Stationery Office, 2009. http://www.official-documents.gov.uk/document/cm75/7590/7590.pdf.

———. *The National Security Strategy: A Strong Britain in an Age of Uncertainty*. Norwich: The Stationary Office, 2010.

———. 'Office of Cyber Security and Information Assurance (OCSIA).' http://www.cabinetoffice.gov.uk/content/office-cyber-security-and-information-assurance-ocsia.

———. 'Risk Assessment.' UK Cabinet Office, http://www.cabinetoffice.gov.uk/content/risk-assessment.

———. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. London: UK Cabinet Office, 2011.

UK Home Office. *Cyber Crime Strategy*. Norwich: The Stationery Office, 2010.

UK Security Service (MI5). 'Protecting National Security.' https://www.mi5.gov.uk/home/about-us/what-we-do/protecting-national-security.html.

UNDP. *Human Development Report 1994. New Dimensions of Human Security*. Oxford and New York: Oxford University Press, 1994. http://hdr.undp.org/en/reports/global/hdr1994.

UNGA. *Definition of Aggression (A/RES/3314(XXIX))*. New York: United Nations, 1974.

———. *Developments in the field of information and telecommunications in the context of international security (A/RES/66/24)*. New York: United Nations, 2011.

———. *Developments in the field of information and telecommunications in the context of*

*international security. Report of the Secretary-General (A/66/152/Add.1)*. New York: United Nations, 2011.

———. *International Convention for the Suppression of Acts of Nuclear Terrorism (A/59/766)*. New York: United Nations, 2005.

———. *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)*. New York: United Nations, 2011.

———. *The United Nations Global Counter-Terrorism Strategy (A/RES/60/288)*. New York: United Nations, 2006.

UNISDR. 'Terminology.' http://www.unisdr.org/we/inform/terminology.

United Nations. *Charter of the United Nations*. San Fransisco, CA: United Nations, 1945.

———. *The Statute of the International Court of Justice*. San Francisco, CA: United Nations, 1945.

———. *Vienna Convention on Diplomatic Relations*. Vienna: United Nations, 1961.

———. *Vienna Convention on the Law of Treaties*. Vienna: United Nations, 1969.

United States, *et al. North Atlantic Treaty*. Washington, DC: NATO, 1949.

International Court of Justice. *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*. ICJ Reports 1981, 64.

UNODA. 'Developments in the field of information and telecommunications in the context of international security.' United Nations, http://www.un.org/disarmament/topics/informationsecurity.

UNSG. *Secretary-General's Bulletin: Observance by United Nations Forces of International Humanitarian Law (ST/SGB/1999/13)*. New York: United Nations, 1999.

US Department of Commerce. *Cybersecurity, Innovation, and the Internet Economy (Green Paper)*. Gaithersburg, MD: NIST, 2011. http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

US Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC 2011.

US Department of Homeland Security. *DHS Risk Lexicon*. Washington, DC: Risk Steering Committee, 2008. http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf.

———. *Joint Statement by Secretary of Defense Robert Gates and Secretary of Homeland Security Janet Napolitano on Enhancing Coordination to Secure America's Cyber Networks*. Washington, DC 2010.

———. *National Incident Management System*. Washington, DC: FEMA, 2008. http://www.

fema.gov/pdf/emergency/nims/NIMS_core.pdf.

———. 'United States and India Sign Cybersecurity Agreement.' *Office of the Press Secretary*, 19 July 2011.

US DoC/NIST. *Minimum Security Requirements for Federal Information and Information Systems*. Gaithersburg, MD: NIST, 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

US Government. 'Using Goals to Improve Performance and Accountability.' Performance.gov, http://goals.performance.gov/goals_2013.

US Government Accountability Office. *Cyberspace. United States Faces Challenges in Addressing Global Cybersecurity and Governance*. Washington, DC: US Government Accountability Office, 2010. http://gao.gov/assets/310/308401.pdf.

US Joint Chiefs of Staff. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. Ft. Belvoir, VA: DTIC, 2012. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

———. *Joint Publication 3-13. Information Operations*. Ft. Belvoir, VA: DTIC, 2006. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

———. *Joint Publication 6-0. Joint Communications System*. Ft. Belvoir, VA: DTIC, 2010. http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

US National Security Council. *NSC 68: United States Objectives and Programs for National Security*. Washington, DC: FAS, 1950.

US Nuclear Regulatory Commission. *Regulatory Guide 5.71. Cyber Security Programs for Nuclear Facilities*. Washington, DC: US Nuclear Regulatory Commission, 2010.

US Office of the National Counterintelligence Executive. *Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*. Washington, DC: US Office of the National Counterintelligence Executive, 2011. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

US Senate Committee on Armed Services. *Statement of General Keith B. Alexander, Commander United States Cyber Command*, 27 March 2012.

Verizon. *2012 Data Breach Investigations Report*. Arlington, VA: Verizon Business, 2012. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

Walt, Stephen M. 'Who is full of hot air on climate change?' *Foreign Policy*, 23 July 2012.

Walton, Timothy. 'Treble Spyglass, Treble Spear?: China's Three Warfares.' *Defense Concepts* 4, no. 4 (2009): 49-65.

WARP. 'WARP – Protecting our information infrastructures.' CPNI, http://www.warp.gov.uk.

Warren, Peter. 'Hunt for Russia's web criminals.' *The Guardian*, 15 November 2007.

Waugh, Tim. 'Berlin Plus agreement.' European Parliament, http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/berlinplus_/berlinplus_en.pdf.

White House. *The Comprehensive National Cybersecurity Initiative (as codified in NSPD-54/HSPD-23)*. Washington, DC: White House, 2008.

———. *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC: White House, 2009.

———. *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*. Washington, DC 2011.

———. 'Joint Fact Sheet: U.S.-UK Progress Towards a Freer and More Secure Cyberspace.' *Office of the Press Secretary*, 14 March 2012.

———. *National Security Strategy*. Washington, DC: White House, 2010.

———. *The National Strategy to Secure Cyberspace*. Washington, DC: White House, 2003.

Williams, Christopher. 'How Egypt shut down the internet.' *The Telegraph*, 28 January 2011.

WSIS. *Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E)*. Tunis: ITU, 2005.

Zeenews. 'US, China, Russia have 'cyber weapons': McAfee.' *Zeenews.com*, 18 November 2009.

Zeltser, Lenny. 'The Big Picture of the Security Incident Cycle.' *Computer Forensics and Incident Response*, 27 September 2010.

Zhao, Xiaofan. 'Practice and Strategy of Informatization in China.' Shanghai: UPAN, 2006.

# GLOSSARY

## A

| | |
|---|---|
| AFIWC | Air Force Information Warfare Center (US) |
| ANG | Air National Guard (US) |
| ANSSI | French Network and Information Security Agency (Agence Nationale de la Sécurité des Systèmes d'Information) (RF) |
| APT | Advanced Persistent Threat |
| ARPANET | Advanced Research Projects Agency Network (US) |
| ARSTRAT | Army Forces Strategic Command (US) |

## B

| | |
|---|---|
| BGP | Border Gateway Protocol |

## C

| | |
|---|---|
| C2 | Command and Control (US Army) |
| C4SIR | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (NATO) |
| CCIPS | Computer Crime & Intellectual Property Section |
| CCP | Chinese Communist Party |
| CCTV | Closed Circuit Television |
| CDR | Commander |
| CEO | Chief Executive Officer |
| CERT | Computer Emergency Response Teams |
| CERTA | Technical component of COSSI (Unité Technique et Intervention) (RF) |
| CERT/CC | CERT Coordination Center |
| CEVECS | Situational analysis and early warning centre (CEntre VEille Conduite Synthèses) (RF) |
| CHCSS | Chief, Central Security Service (US-NSA) |
| CI | Critical Infrastructure |
| CIA | Central Intelligence Agency (US) |
| C-I-A | Confidentiality, Integrity, Availability |

| | |
|---|---|
| CIIP | Critical Information Infrastructure Protection |
| CIP | Critical Infrastructure Protection |
| CMC | Central Military Commission (PRC) |
| CNA | Computer Network Attack |
| CNCI | Comprehensive National Cybersecurity Initiative |
| CND | Computer Network Defence |
| CNE | Computer Network Exploitation |
| CNO | Computer Network Operations |
| COPS | (see PSC) |
| COREPER | Committee of Permanent Representatives (EU) |
| COSI | Committee on operational cooperation on internal security |
| COSSI | French Operational Center of the Security of Information Systems (Centre Opérationnel en Sécurité des Systèmes d'Informations) (RF) |
| CSC | Council Security Committee (INFOSEC) (EU) |
| CSIRT | Computer Security Incident Response Teams |
| CSIS | Centre for Strategic and International Studies |
| CSR | Cyber Security Council (NL) |
| CSS | Central Security Service (US-NSA) |
| CSSP | Control Systems Security Program |
| CTCPEC | Canadian Trusted Computer Product Evaluation Criteria |
| CYBERCOM | US Cyber Command |

## D

| | |
|---|---|
| DARPA | Defense Advanced Research Projects Agency (US) |
| DC3 | Department of Defense Cybercrime Center (US) |
| DDoS | Distributed Denial of Service |
| DG | Directorate General (EU) |
| DHS | Department of Homeland Security (US) |
| DIA | Defense Intelligence Agency (US) |
| DiB | Defense Industrial Base (US) |
| DIME | Diplomatic, Information, Military and Economic |
| DIRDISA | Director, Defense Information Systems Agency (US) |

| | |
|---|---|
| DISA | Defense Information Systems Agency (US) |
| DNS | Domain Name System |
| DoD | Department of Defense (US) |
| DodIIS | Department of Defense Intelligence Information Systems (US) |
| DOJ | Department of Justice (US) |
| DoS | Denial of Service |

## E

| | |
|---|---|
| EBAO | Effect Based Approach to Operations |
| EC | European Commission (EC) |
| EFF | Electronic Frontier Foundation |
| ELINT | Electronic Intelligence |
| EU | European Union |
| EUMC | EU Military Committee |

## F

| | |
|---|---|
| FAPSI | Federal Agency of Government Communications and Information (RF) |
| FBI | Federal Bureau of Investigation (US) |
| FEP | Effective Politics Foundation (RF) |
| FIRST | Forum of Incident Response and Security Teams |
| FISMA | Federal Information Security Management Act (US) |
| FIWC | Fleet Information Warfare Centre |
| FSB | Federal Security Service of the Russian Federation |
| FS-ISAC | Financial Services Information Sharing and Analysis Center (US) |
| FSO | Federal Protective Service (RF) |

## G

| | |
|---|---|
| G8 | Group of Eight |
| GAO | General Accountability Office (US Congress) |
| Gbits/s | Gigabits per second |
| GBP | Great Britain Pound |

| | |
|---|---|
| GCHQ | Government Communications Headquarters (UK) |
| GIG | Global Information Grid |
| GNEC | Global Network Enterprise Construct |
| GRU | Russian military intelligence |
| GSD | General Staff Department (PRC) |
| GUO | Russia Main Guard Directorate, predecessor of FSO |
| GUSTM | Main Directorate for Special Technical Measures (RF) |

## H

| | |
|---|---|
| HSPD | Homeland Security Presidential Directive |
| HUMINT | Human Intelligence |

## I

| | |
|---|---|
| IC | Intelligence Community (US) |
| IC3 | Internet Crime Complaints Center (US) |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IC-IRC | Intelligence Community-Incident Response Center (US) |
| ICMP | Internet Control Message Protocol |
| ICS | Industrial Control System |
| ICT | Information and Communications Technology |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IGF | Internet Governance Forum |
| INC | Integrated National Capability |
| I-NOSC | Integrated Network and Operations Center (US) |
| INSCOM | Intelligence and Security Command (US) |
| IO | Information Operations |
| IP | Internet Protocol |
| ISACs | Information Sharing and Analysis Centers (US) |
| ISO | Information Security Standard |
| ISP | Internet Service Provider |

| | |
|---|---|
| IT | Information Technology |
| ITSEC | Information Technology Security Evaluation Criteria |
| ITU | International Telecommunications Union |
| IW | Information Warfare |
| IXP | Internet Exchange Points |

## J

| | |
|---|---|
| JFCC-NW | Joint Function Component Command – Network Warfare |
| JIOWC | Joint Information Operations Warfare Center (US) |
| JP | Joint Publications (US) |
| JTF-GNO | Joint Task Force Global Network Operations |

## K

| | |
|---|---|
| KSB | Kremlin School of Bloggers |

## L

| | |
|---|---|
| LAN | Local Area Network |
| LSE | London School of Economics |
| LSZ Centre | Centre for Licensing, Certification and Protection of State Secrets (RF) |

## M

| | |
|---|---|
| Mbits/s | Megabits per second |
| MCNOSC | Marine Corps Network Operations and Security Center (US) |
| MELANI | Reporting and Analysis Centre for Information Assurance (CH) |
| MILDEC | Military Deception |
| MSS | Ministry of State Security (PRC) |
| MVD | Ministry of Internal Affairs (RF) |

## N

| | |
|---|---|
| NAC | National Antiterrorism Centre (RF) |
| NATO | North Atlantic Treaty Organisation |
| NCCT | Network Centric Collaborative Targeting |

| | |
|---|---|
| NCDOC | Navy Cyber Defense Operations Command (US) |
| NCI-JTF | National Cyber Investigative Joint Task Force (US) |
| NCO (W) | Network Centred Operations (Warfare) |
| NCPH | Network Crack Program Hacker |
| NCRCG | National Cyber Response Coordination Group |
| NCS | National Cyber Security |
| NCSC | National Cybersecurity Center (US) |
| NCSD | National Cybersecurity Division (US) |
| NCSS | National Cyber Security Strategies |
| NCW | Network Centric Warfare |
| NMS | National Military Strategy (US) |
| NNWC | Naval Network Warfare Command (US) |
| NSA | National Security Agency (US) |
| NSCC | National Strategy to Secure Cyberspace (US) |
| NSPD | National Security Presidential Directive |
| NSP-SEC | Network Service Provider Security (EE) |
| NTOC | NSA/CSS Threat Operations Center (US) |

## O

| | |
|---|---|
| OECD | Organisation for Economic Co-operation and Development |
| oiip | Österreichisches Institut für Internationale Politik |
| OPSEC | Operational Security |
| OSCE | Organisation for Security and Cooperation in Europe |
| OSINT | Open Source Intelligence Investigators |

## P

| | |
|---|---|
| P2P | Peer-to-peer |
| PDD | Presidential Decision Directive (US) |
| PDoS | Permanent Denial of Service |
| PIRANET | French national cyber crisis management plan |
| PLA | People's Liberation Army (PRC) |

| | |
|---|---|
| PLAF | People's Liberation Armed Forces (PRC) |
| PLAN | People's Liberation Army Navy (PRC) |
| PRC | People's Republic of China |
| PSB | Public Security Bureau (PRC) |
| PSC | Political and Security Committee (EU) |
| PSYOPS | Psychological Operations |

## R

| | |
|---|---|
| R&D | Research and Development |
| RAND | Research and Development – Corporation (US) |
| RBN | Russian Business Network |
| RCERTs | Regional Computer Emergency Response Teams |
| RF | Russian Federation |
| RMA | Revolution in Military Affairs (PRC) |
| RNOSCs | Regional Network Operations and Security Centers (US) |
| RSSC | Regional SATCOM Support Centres |

## S

| | |
|---|---|
| SCADA | Supervisory Control and Data Acquisition |
| SHAPE | Supreme Headquarters Allied Powers Europe |
| SIGINT | Signals Intelligence |
| SITCEN | Situation Centre (EU) |
| SIUN | A committee subordinate to the Government responsible for assuring that all interception is done according to the Swedish law (Statens inspektion för försvarsunderrättelseverksamheten) (SE) |
| SME | Small and Medium Size Enterprise |
| SORM | System for Operative Investigative Activities (RF) |
| SQL | Structured Query Language |
| STN | Security Trust Networks |
| SVR | Foreign Intelligence Service (RF) |

## T

| | |
|---|---|
| TCP/IP | Transmission Control Protocol/ Internet Protocol |
| TCSEC | Trusted Computer System Evaluation Criteria |
| Telnet | Telecommunication Network |
| TOC | Tactical Operations Centre |
| TR-NOCS | Theatre Regional Network Operations Center (US) |
| TTP | Tactical Techniques and Procedures (US Army) |

## U

| | |
|---|---|
| UK | United Kingdom |
| UNIDIR | United Nations Institute for Disarmament Research |
| UP-BUND | IT security guidelines for the federal authorities (GER) |
| UP-KRITIS | IT security guidelines for the private sector (GER) |
| US | United States |
| USAF | United States Air Force |
| USD | United States Dollar |
| USSTRATCOM | United States Strategic Command |

## V

| | |
|---|---|
| VoIP | Voice over Internet Protocol |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WARP | Warning, Advice and Reporting Point |
| WLAN | Wireless Local Area Network |
| WoG | Whole of Government |
| WoN | Whole of Nation |
| WoS | Whole of System |

# AUTHORS' BIOGRAPHIES

**Dave Clemente** is a Researcher with International Security at the Royal Institute of International Affairs (Chatham House). His areas of expertise include cyber security policy and US and UK security and defence policy. He has worked at the International Institute for Strategic Studies and the Overseas Development Institute. He is the author of *Cyber Security and Global Interdependence* (Chatham House, 2012) and co-author of *Cyber Security and the UK's Critical National Infrastructur*e (Chatham House, 2011) and *On Cyber Warfare* (Chatham House, 2010).

**Victoria Ekstedt** has been the principal legal adviser for the Swedish Armed Forces Computer Network Operations Unit since 2007. She holds a Master of Law degree specialised in international Law from the Uppsala University, Sweden, and a Masters degree in Commercial and Maritime Law from the University of Southampton, England. Ms Ekstedt has practiced commercial law within the Swedish defence industry and served as legal adviser and military judge to the armed forces in Bosnia-Herzegovina in 2004 and 2005. She is also a former military officer of the 1st Amphibious Regiment of the Swedish Armed Forces.

**Melissa Hathaway** is President of Hathaway Global Strategies, LLC and a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs to its cyber security initiative, Project Minerva. Ms Hathaway served in the Obama Administration as Acting Senior Director for Cyberspace at the National Security Council and led the Cyberspace Policy Review. During the last two years of the administration of George W. Bush, Ms Hathaway served as Cyber Coordination Executive and Director of the Joint Interagency Cyber Task Force in the Office of the Director of National Intelligence where she led the development of the Comprehensive National Cybersecurity Initiative (CNCI). At the conclusion of her government service she received the National Intelligence Reform Medal and the National Intelligence Meritorious Unit Citation in recognition of her achievements. Previous to joining the government, Ms Hathaway held positions in Booz Allen Hamilton and is known for her long range strategy development and policy formulation and cyber security expertise. She has a B.A. degree from The American University in International Relations and Government. She also has completed graduate studies in international economics and technology transfer policy and is a graduate of the US Armed Forces Staff College, with a special certificate in Information Operations.

**Jason Healey** is the Director of the Cyber Statecraft Initiative of the Atlantic Council, focusing on international cooperation, competition and conflict in cyberspace. He also is a board member (and former Executive Director) of the Cyber Conflict Studies Association and lecturer in cyber policy at Georgetown University. He is

the principal investigator in the first book on cyber conflict history and his ideas on cyber topics have been widely published. As Director for Cyber Infrastructure Protection at the White House from 2003 to 2005, he helped advise the President and coordinated US efforts to secure US cyberspace and critical infrastructure. He also worked for Goldman Sachs where, as Executive Director he was responsible for developing the bank's regional crisis management and business continuity capabilities.

**Alexander Klimburg** is Fellow and Senior Adviser at the Austrian Institute for International Affairs. Since joining the Institute in October 2006, Mr Klimburg has acted as an adviser to governments and international organizations on a number of issues within cyber security, Critical Infrastructure Protection (CIP), and EU Common and Foreign Security Policy (CFSP). Mr Klimburg has partaken in international and intergovernmental discussions, has acted as an advisor to the Austrian delegation at the OSCE, and has been a member of various national and EU-level policy and working groups. Together with Heli Tiirmaa-Klaar he is the author of a 2011 European Parliament study entitled *Cyberpower and Cybersecurity,* and regularly advises on cyber security legislation. Within cyber security, Mr Klimburg's work has primarily been in the area of Information Security, Critical (Information) Infrastructure Protection, and researching the synthesis of different types of cyber security issues in exercising 'cyberpower'. Mr Klimburg is particularly interested in the roles that non-state actors have within cyber security, and how these roles can contribute to a whole-of-nation 'Integrated National Capability' within cyberpower. Mr Klimburg is the author of a number of advisory papers and is regularly consulted by national and international media. Previous to joining the institute, Mr Klimburg worked on ICT strategy issues in corporate finance and IT/strategy consulting in Europe and Asia, and he holds degrees from the School of Oriental and African Studies and the London School of Economics and Political Science.

**Gustav Lindstrom** is the Head of the Emerging Security Challenges Programme at the Geneva Centre for Security Policy (GCSP). He received his doctorate in Policy Analysis from the RAND Graduate School (Santa Monica, California) and a M.A. in International Policy Studies from Stanford University (Palo Alto, California). Prior to his tenure at the GCSP, Dr Lindstrom served as a Senior Research Fellow at the EU Institute for Security Studies. His publications cover a wide range of issues relating to international security – including transatlantic relations, Common Foreign and Security Policy of the EU, terrorism, non-proliferation, the strategic use of outer space, and cyber security.

**Eric Luiijf** M.Sc (Eng) Delft works as Principal Consultant Critical Infrastructure Protection and Information Operations at the Netherlands Organisation for Applied Scientific Research TNO, The Hague, the Netherlands. He supports the Dutch

Government on policy-related issues regarding Critical (Information) Infrastructure Protection (C(I)IP) and Information Operations/Warfare. He has been involved in many EU studies on CIP and CIIP research and development. Example projects are the policy studies on the vulnerability of the Dutch internet (KWINT), the Quick-Scan on Dutch Critical Infrastructure, (in)security of Process Control Systems, the development of a Good Practice book for CIP Policy-makers (RECIPE). Mr Luiijf participates in multiple NATO research task groups on Cyber Defence and leads an international exploratory team in this domain; he is an expert member in the Dutch Centre for the Protection of National Infrastructure (CPNI.NL) driving the Process Control System Security initiatives such as good practices and critical sector benchmarks. He is one of the founders and editors of the European CIIP newsletter. Mr Luiijf has published many popular articles, reports, and scientific publications about cyber terrorism, critical (information) infrastructure protection, and information assurance.

**Tom Parkhouse** is a Senior Fellow of the Cyber Statecraft Initiative of the Atlantic Council with a particular interest in the integration of cyber issues into Governmental policy. He is a former member of the Royal Air Force Police with broad security and counter-intelligence experience. Between 2008 and 2012 he served in various Ministry of Defence appointments focussed on cyber issues and was a key contributor to the first UK National Cyber Security Strategy, and a member of the Working Group that oversaw the development of the UK Cyber Security Operation Centre. Following the 2010 Strategic Defence and Security Review, Mr Parkhouse served as a member of the implementation team for the Defence Cyber Operations Group. He holds degrees from the Royal Military College of Science (Information Systems Management) and Kings College London (Military Studies); he is also a Certified Information Systems Security Professional.

What, exactly, is 'national cyber security'? The rise of cyberspace as a field of human endeavour is probably nothing less than one of the most significant developments in world history. Cyberspace already directly impacts every facet of human existence including economic, social, cultural and political developments, and the rate of change is not likely to stop anytime soon. However, the socio-political answers to the questions posed by the rise of cyberspace often significantly lag behind the rate of technological change. One of the fields most challenged by this development is that of national security.

The term 'national cyber security' is increasingly used when discussing the overall security challenges nation-states face in cyberspace, but it is seldom defined. Overall, the individual national context will determine the specific definitions and approaches governments will take when seeking to balance the social-economic gains of information technology with the new security risks that accompany it. Understanding the specific national context, therefore, is key to developing an appropriate national strategy.

Accordingly, the 'National Cyber Security Framework Manual' does not simply strive to provide a single universally applicable checklist of aspects to consider when drafting a national cyber security strategy. Rather, it provides detailed background information and in-depth theoretical frameworks to help the reader understand the different facets of national cyber security, according to different levels of public policy formulation. The four levels of government – political, strategic, operational and tactical/technical – each have their own perspectives on national cyber security, and each is addressed in individual sections within the Manual. Additionally, the Manual gives examples of relevant institutions in national cyber security, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions. The Manual can thus be read as a collective volume or on a section-by-section basis, according to the needs of the reader.

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia